-----((الفصل الرابع))-----

تثبيت Kali Linux

في هذا الفصل، سوف نركز على عملية تثبيت Kali Linux. أولاً، سنناقش الحد الأدنى لمتطلبات التثبيت (الباب ٤.١. "الحد الأدنى لمتطلبات التثبيت") للتأكد من أن نظامك الحقيقي أو الافتراضي قد تم تهيئته بشكل جيد للتعامل مع نوع التثبيت الذي ستتبعه. بعد ذلك، سوف نمر بكل خطوة من خطوات عملية التثبيت (الباب ٤.٢. "التثبيت خطوة بخطوة على القرص الصلب") للتثبيت العادي، وكذلك للتثبيت الأكثر أمانًا الذي يتضمن نظام ملفات مشفر بالكامل.

سوف نناقش أيضًا مرحلة ما *قبل التثبيت* "preseeding"، والتي تسمح بالتثبيتات غير المراقبة (الباب ٤.٣. "التثبيتات الغير مراقبة") من خلال تقديم إجابات محددة مسبقًا على أسئلة التثبيت. سنبين لك أيضًا كيفية تثبيت Kali Linux على أجهزة ARM المختلفة (الباب ٤.٤. "تثبيتات ARM")، مما يوسع قدرات Kali إلى أبعد من سطح مكتب. أخيرًا، سوف نوضح لك ما يجب القيام به في حالة نادرة فشل التثبيت (الباب ٤.٥. "استكشاف أخطاء التثبيتات")، حتى تتمكن من حل المشكلة وإنهاء عملية تثبيت صعبة بنجاح.

١.٤. الحد الأدنى لمتطلبات التثبيت

تختلف متطلبات التثبيت لـ Kali Linux حسب ما تريد تثبيته. على الطرف الأدنى، يمكنك إعداد Kali كخادم Secure Shell (SSH) أساسي بدون سطح مكتب، باستخدام ذاكرة وصول عشوائي (RAM) لا تقل عن ١٢٨ ميجابايت (يوصى باستخدام ٥١٢ ميجابايت) و٢ جيجابايت من مساحة القرص. في النهاية العليا، إذا اخترت تثبيت سطح مكتب GNOME الافتراضي وحزمة التعريف kali-linux-full، فيجب أن تحصل على 2048 MB على الأقل من ذاكرة الوصول العشوائي و20 GB من مساحة القرص.

إلى جانب متطلبات ذاكرة الوصول العشوائي والأقراص الصلبة، يحتاج الحاسوب لديك إلى وحدة المعالجة المركزية مدعومة على الأقل من بنيات amd64 أو i386 أو armel أو armhf أو arm64.

٢.٤. التثبيت خطوة بخطوة على القرص الصلب

في هذا الباب، نفترض أن لديك محرك أقراص USB أو قرص DVD قابلًا للإقلاع (راجع الباب ٤.١.٢. "نسخ الصورة على قرص DVD-ROM أو مفتاح USB" للحصول على تفاصيل حول كيفية إعداد محرك الأقراص هذا) وأنك قمت بالإقلاع منه لبدء عملية التثبيت.

١.٢.٤. تثبيت عادي

أولاً، سوف نلقي نظرة على تثبيت Kali القياسي، باستخدام نظام ملفات غير مشفر.

١.١.٢.٤. إقلاع وبدء التثبيت

بمجرد بدء BIOS في التشغيل من محرك أقراص USB أو DVD-ROM، تظهر قائمة أداة محمل الإقلاع لصورة لينكس، كما هو مبين في الشكل ١.٤. "شاشة الإقلاع". في هذه المرحلة، لم يتم تحميل نواة لينكس بعد؛ تتيح لك هذه القائمة اختيار نواة للإقلاع وإدخال معلمات اختيارية لنقلها إليه في هذه العملية.

للتثبيت القياسي، ما عليك سوى اختيار install أو Graphical Install (بمفاتيح الأسهم)، ثم اضغط على مفتاح **Enter** لبدء ما تبقى من عملية التثبيت.

يخفي كل إدخال قائمة سطر أوامر إقلاع محددًا، والذي يمكن تهيئته حسب الحاجة عن طريق الضغط على مفتاح **Tab** قبل التحقق من الإدخال والتشغيل.



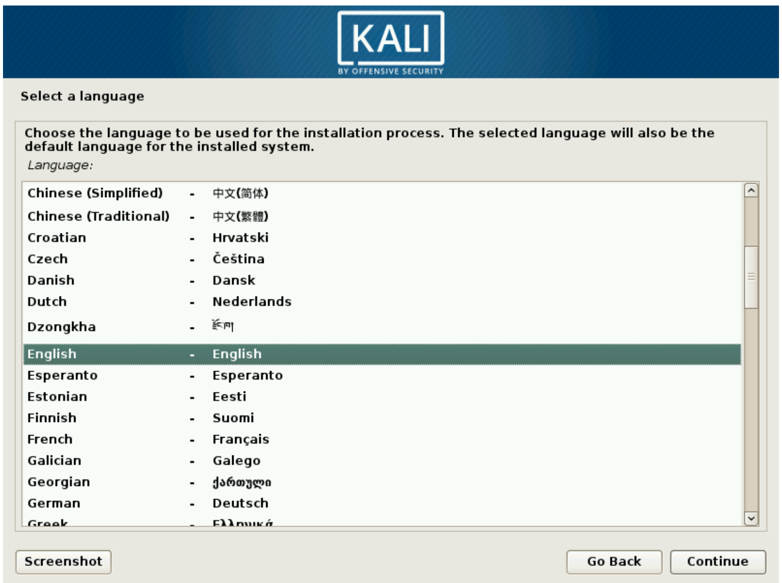
شكل ١.٤. شاشة الإقلاع

بمجرد الإقلاع، يرشدك برنامج التثبيت خطوة بخطوة خلال العملية. سوف نلقي نظرة على كل خطوة من هذه الخطوات بالتفصيل. سنغطي التثبيت من Kali Linux DVD-ROM قياسي؛ المثبتة من **mini.iso** قد تبدو مختلفة بعض الشيء. سنقوم أيضًا بتثبيت الوضع الرسومي، ولكن الفرق الوحيد من تثبيت وضع النص هو المظهر الكلاسيكي.

٤.٢.١.٢. اختيار اللغة

كما هو مبين في الشكل ٤.٢. "اختيار اللغة"، يبدأ برنامج التثبيت باللغة الإنجليزية ولكن الخطوة الأولى تسمح لك باختيار اللغة التي سيتم استخدامها لبقية عملية التثبيت. يتم استخدام اختيار اللغة هذا أيضًا لتحديد الخيارات الافتراضية ذات الصلة في المراحل اللاحقة (لا سيما تخطيط لوحة المفاتيح).

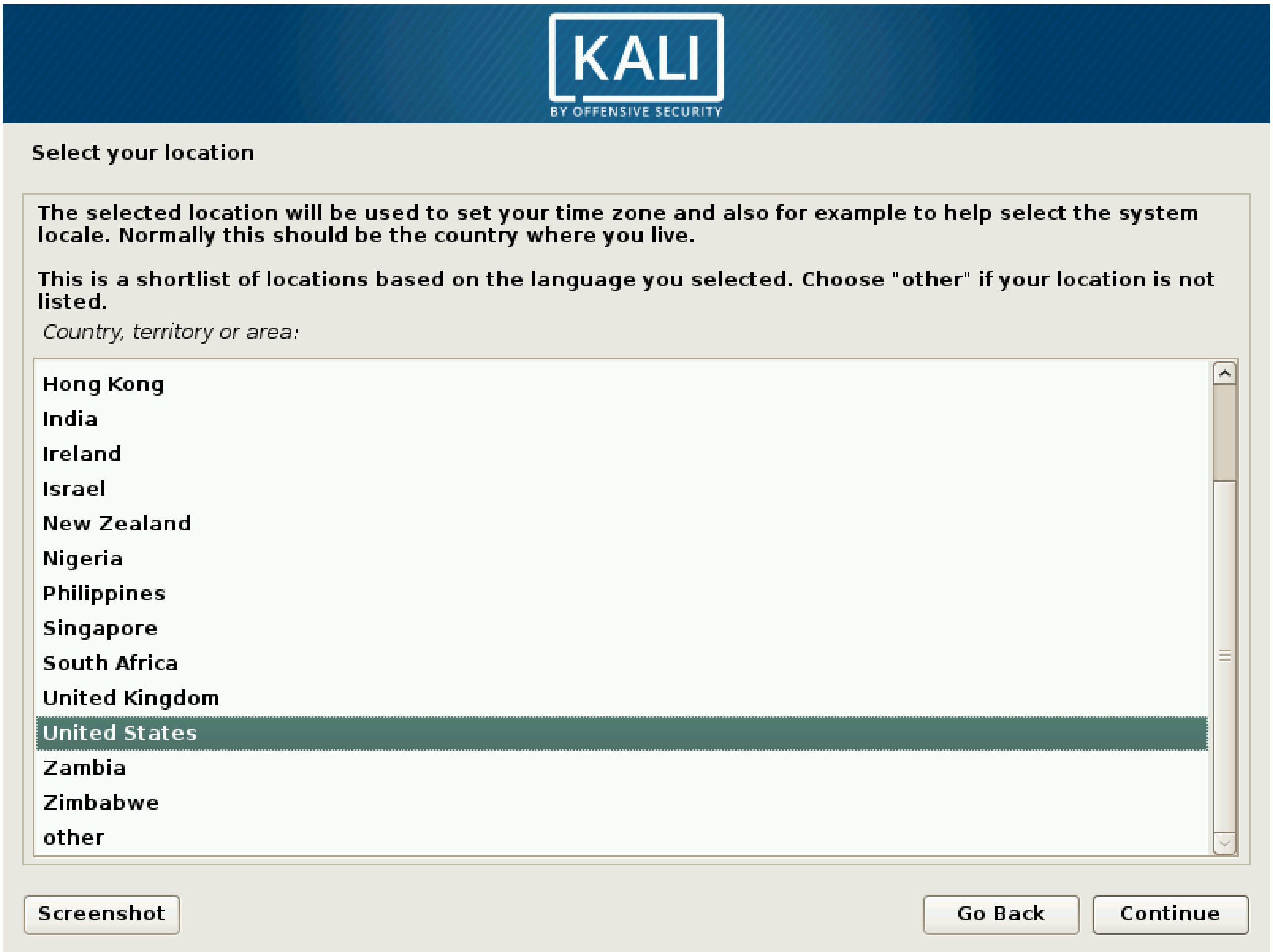
> **التنقل باستخدام لوحة المفاتيح**
>
> تتطلب بعض الخطوات في عملية التثبيت إدخال المعلومات. تحتوي هذه الشاشات على العديد من الخانات التي تريد الإنتقال لها (خانة إدخال النص، وخانات الاختيار، وقائمة الخيارات، وأزرار الموافقة والإلغاء)، يسمح لك مفتاح **Tab** بالانتقال من خانة لإخرى. في وضع التثبيت الرسومي، يمكنك استخدام الماوس كما تفعل عادةً في سطح مكتب رسومي.



شكل ٤.٢. اختيار اللغة

٣.١.٢.٤. اختيار البلد

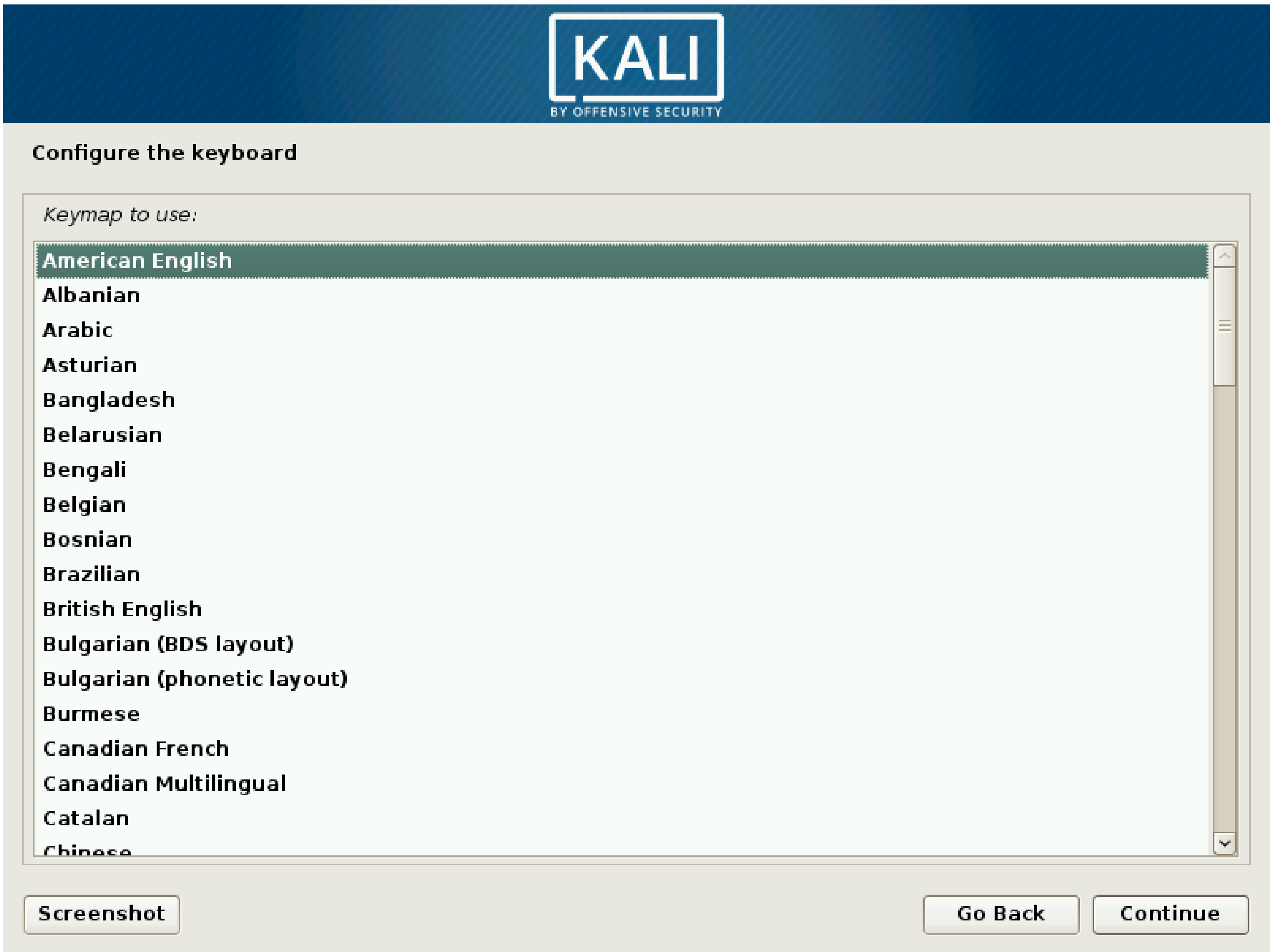
تمثل الخطوة الثانية (الشكل ٣.٤. "اختيار البلد") في اختيار بلدك. بالإضافة إلى اللغة، تُمكّن هذه المعلومات برنامج التثبيت من تقديم تخطيط لوحة المفاتيح الأكثر ملاءمة. سيؤثر هذا أيضًا على تكوين المنطقة الزمنية. في الولايات المتحدة، تُقترح لوحة مفاتيح QWERTY قياسية ويقدم المثبت اختيارًا للمناطق الزمنية المناسبة.



شكل ٣.٤. اختيار البلد

٤.١.٢.٤. اختيار تخطيط لوحة المفاتيح

تتوافق لوحة المفاتيح الإنجليزية الأمريكية المقترحة مع تخطيط QWERTY المعتاد كما هو موضح في الشكل ٤.٤. "اختيار تخطيط لوحة المفاتيح".



شكل ٤.٤. اختيار تخطيط لوحة المفاتيح

٤.٢.١.٥. التعرف على الهاردوير

في الغالبية العظمى من الحالات، تكون خطوة اكتشاف الأجهزة تلقائية بالكامل. يكشف المثبت عن أجهزتك ويحاول تحديد جهاز الإقلاع المستخدم للوصول إلى محتواه. يقوم بتحميل الوحدات المقابلة لمكونات الأجهزة المختلفة المكتشفة، ثم يقوم بوصل جهاز الإقلاع من أجل قراءته. تم تضمين الخطوات السابقة بالكامل في صورة الإقلاع المضمنة في جهاز الإقلاع، وهو ملف ذو حجم محدود ويتم تحميله في الذاكرة بواسطة أداة محمل الإقلاع عند التشغيل من جهاز الإقلاع.

٤.٢.١.٦. تحميل المكونات

مع توفر محتويات جهاز الإقلاع الآن، يقوم المثبت بتحميل جميع الملفات اللازمة لمتابعة عمله. يتضمن ذلك برامج تشغيل إضافية للأجهزة المتبقية (خاصة بطاقة الشبكة)، بالإضافة إلى جميع مكونات برنامج التثبيت.

٤.٢.١.٧. التحقق من هاردوير الشبكة

في هذه الخطوة، سيحاول المثبت تحديد بطاقة الشبكة تلقائيًا وتحميل الوحدة النمطية المقابلة. في حالة فشل الاكتشاف التلقائي، يمكنك تحديد الوحدة النمطية المراد تحميلها يدويًا. إذا فشل كل شيء آخر، يمكنك تحميل وحدة نمطية معينة من جهاز قابل للإزالة. عادة ما تكون هناك حاجة إلى هذا الحل الأخير فقط إذا لم يتم تضمين برنامج التشغيل المناسب في نواة لينكس القياسية، ولكنه متوفر في مكان آخر، مثل موقع الشركة المصنعة على الويب.

يجب أن تكون هذه الخطوة ناجحة تمامًا لعمليات تثبيت الشبكة (مثل تلك التي تمت عند التشغيل من **mini.iso**)، حيث يجب تحميل حزم دبيان من الشبكة.

٤.٢.١.٨. تكوين الشبكة

من أجل أتمتة العملية إلى أقصى حد ممكن، يحاول المثبت تكوين شبكة تلقائي باستخدام بروتوكول تكوين المضيف الحيوي "dynamic host configuration protocol" (DHCP) (لـ IPv4 و IPv6) (for IPv6) and ICMPv6's Neighbor Discovery Protocol ، كما هو مبين في الشكل ٤.٥. "التكوين التلقائي للشبكة ".



شكل ٤.٥. التكوين التلقائي للشبكة

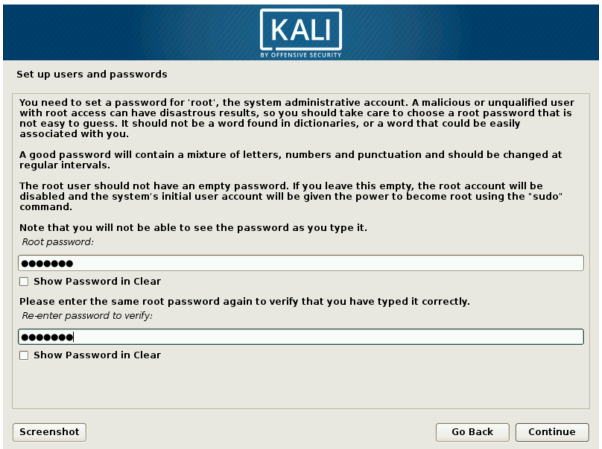
في حالة فشل التكوين التلقائي، يقدم برنامج التثبيت المزيد من الخيارات: حاول مرة أخرى باستخدام تكوين DHCP عادي، أو حاول تكوين DHCP بالإعلان عن اسم الجهاز، أو قم بإعداد تكوين شبكة ثابت. يتطلب هذا الخيار الأخير عنوان IP وقناع شبكة فرعية وعنوان IP للبوابة واسم الجهاز واسم المجال.

التكوين بدون DHCP

إذا كانت الشبكة المحلية مجهزة بخادم DHCP الذي لا ترغب في استخدامه لأنك تفضل تحديد عنوان IP ثابت للجهاز أثناء التثبيت، يمكنك إضافة خيار **`netcfg/use_dhcp=false`** عند التشغيل. تحتاج فقط إلى تحرير إدخال القائمة المطلوبة عن طريق الضغط على مفتاح **Tab** وإضافة الخيار المطلوب قبل الضغط على مفتاح **Enter**.

٩.١.٢.٤. كلمة السر للمستخدم الجذر

يطلب المثبت كلمة مرور (الشكل ٦.٤) لأنه يقوم تلقائيًا بإنشاء حساب جذر للمستخدم الفائق. يطلب المثبت أيضًا تأكيد كلمة المرور لمنع أي خطأ في الإدخال يصعب ضبطه لاحقًا.



شكل ٦.٤. كلمة مرور المستخدم الجذر

كلمة مرور المسؤول

يجب أن تكون كلمة مرور المستخدم الجذر طويلة (ثمانية أحرف أو أكثر) ولا يمكن تخمينها، لأن المهاجمين يستهدفون أجهزة الحاسوب والخوادم المتصلة بالإنترنت باستخدام أدوات آلية، ومحاولة تسجيل الدخول بكلمات مرور واضحة. يستفيد المهاجمون أحيانًا هجمات القاموس، وذلك باستخدام العديد من مجموعات الكلمات والأرقام وكلمات مرور. تجنب استخدام أسماء الأطفال أو الوالدين وتواريخ الميلاد، لأن هذه يسهل تخمينها.

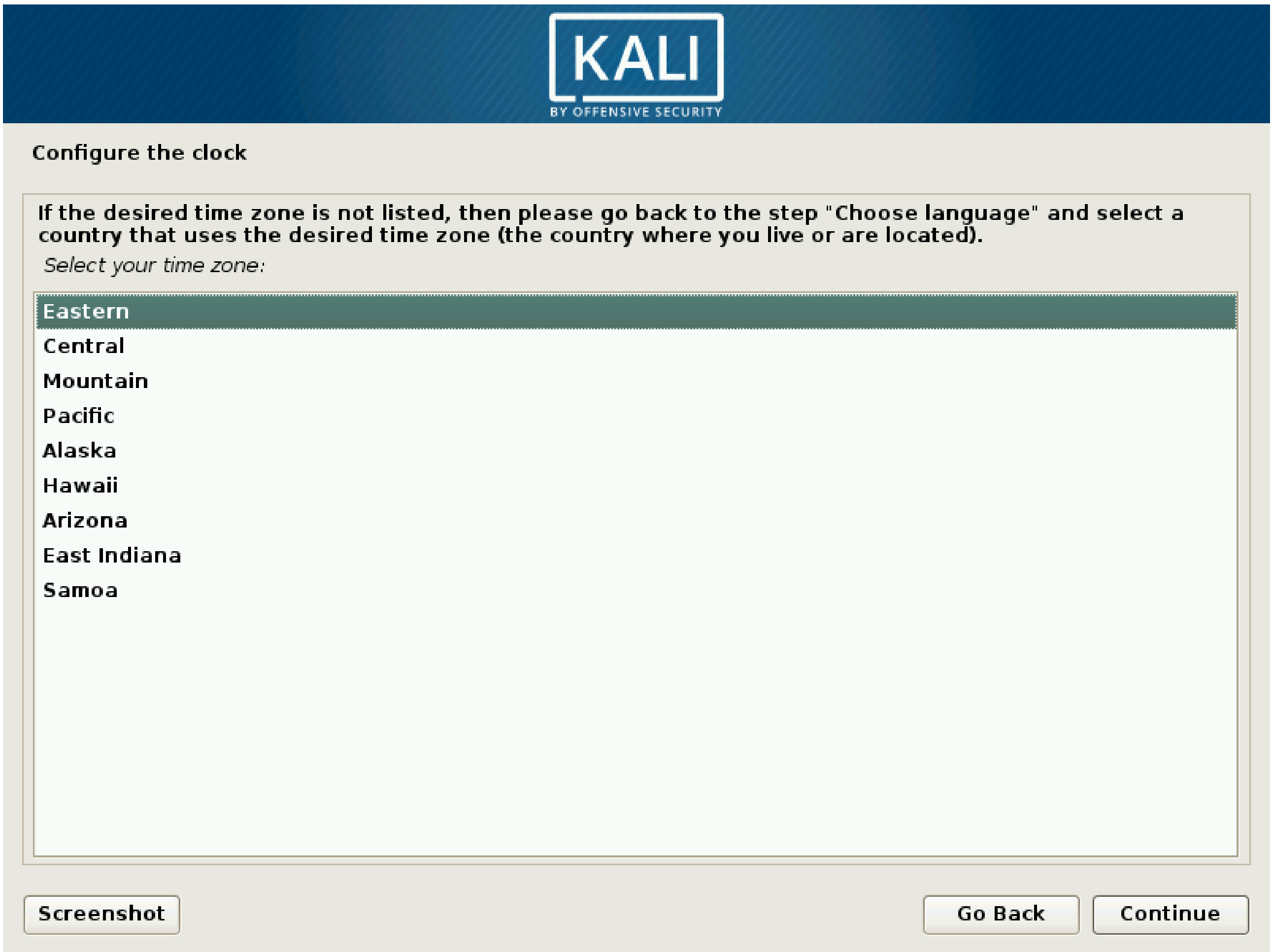
تنطبق هذه الملاحظات بالتساوي على كلمات مرور المستخدمين الأخرى، لكن عواقب حساب مخترق تكون أقل حدة للمستخدمين دون حقوق إدارية.

إذا كنت تفتقر إلى الإلهام، فلا تتردد في استخدام مولد كلمات المرور، مثل **pwgen** (الموجود في الحزمة التي تحمل الاسم نفسه، والمضمنة بالفعل في تثبيت Kali الأساسي).

٤.٢.١.١٠. تكوين الساعة

إذا كانت الشبكة متوفرة، سيتم تحديث الساعة الداخلية للنظام من خادم بروتوكول وقت الشبكة (NTP). يعد هذا مفيدًا لأنه يضمن أن الطوابع الزمنية على السجلات ستكون صحيحة من الإقلاع الأول.

إذا امتد بلدك إلى مناطق زمنية متعددة، فسيُطلب منك تحديد المنطقة الزمنية التي تريد استخدامها، كما هو موضح في الشكل ٤.٧ "تحديد المنطقة الزمنية".



شكل ٤.٧. تحديد المنطقة الزمنية

٤.٢.١.١١. اكتشاف الأقراص والأجهزة الأخرى

تكتشف هذه الخطوة تلقائيًا محركات الأقراص الثابتة التي يمكن تثبيت Kali عليها، وسيتم تقديم كل منها في الخطوة التالية: التقسيم (partitioning).

٤.٢.١.١٢. التقسيم

التقسيم هو خطوة لا غنى عنها في التثبيت، والتي تتكون من تقسيم المساحة المتوفرة على محركات الأقراص الصلبة إلى أقسام منفصلة (*partitions*) وفقًا للوظيفة المقصودة للحاسوب وتلك الأقسام. يتضمن التقسيم أيضًا اختيار أنظمة الملفات المراد استخدامها. جميع هذه القرارات سيكون لها تأثير على الأداء، وأمن البيانات، وإدارة الخادم.

تعتبر خطوة التقسيم صعبة تقليدياً للمستخدمين الجدد. ومع ذلك، يجب تعريف أنظمة ملفات Linux والأقسام، بما في ذلك الذاكرة الافتراضية (أو أقسام المبادلة) لأنها تشكل أساس النظام. يمكن أن تصبح هذه المهمة معقدة إذا كنت قد قمت بالفعل بتثبيت نظام تشغيل آخر على الجهاز وتريد الحفاظ عليهما الاثنان. في هذه الحالة، يجب عليك التأكد من عدم تغيير أقسامهم، أو تغيير حجمهم إذا لزم الأمر دون التسبب في ضرر.

لفهم أوضاع التقسيم الأكثر شيوعًا (والأكثر بساطة)، يفضل معظم المستخدمين وضع الإرشاد *"Guided"* الذي يوصي بتكوينات القسم ويقدم اقتراحات في كل خطوة على الطريق. سيقدر المستخدمون الأكثر تقدماً الوضع اليدوي *"Manual"*، الذي يسمح بمزيد من التكوينات المتقدمة. يشارك كل وضع بعض القدرات.

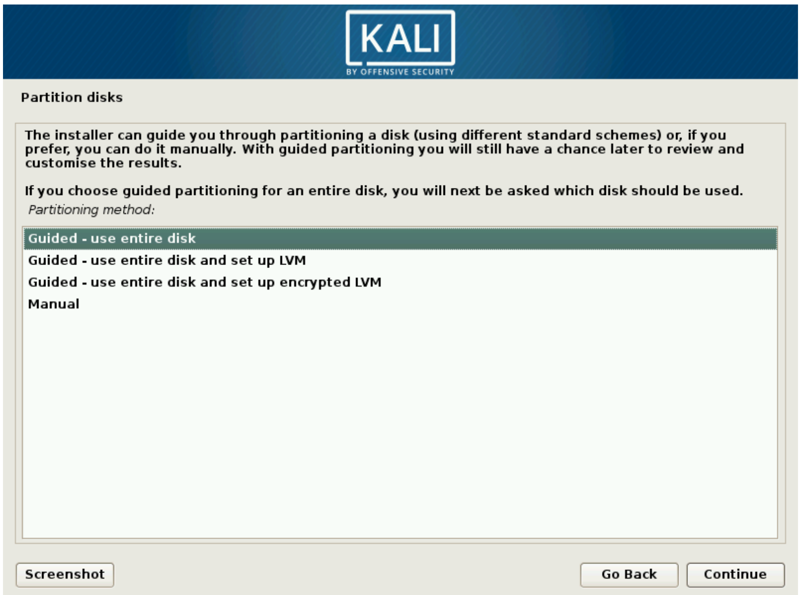
١.١٢.١.٢.٤. التقسيم الموجة

تعرض الشاشة الأولى في أداة التقسيم (الشكل ٨.٤ "اختيار وضع التقسيم") نقاط الدخول لأوضاع التقسيم الموجهة واليدوية. إن "إرشادات استخدام القرص بأكمله (Guided – use entire disk)" هو نظام التقسيم الأسهل والأكثر شيوعًا، والذي سيخصص قرصًا كاملًا لنظام Kali Linux.

يستخدم التحديدان التاليان Logical Volume Manager (LVM) لإعداد أقسام منطقية (بدلاً من المادية)، مشفرة اختيارياً. سنناقش LVM والتشفير لاحقًا في هذا الفصل.

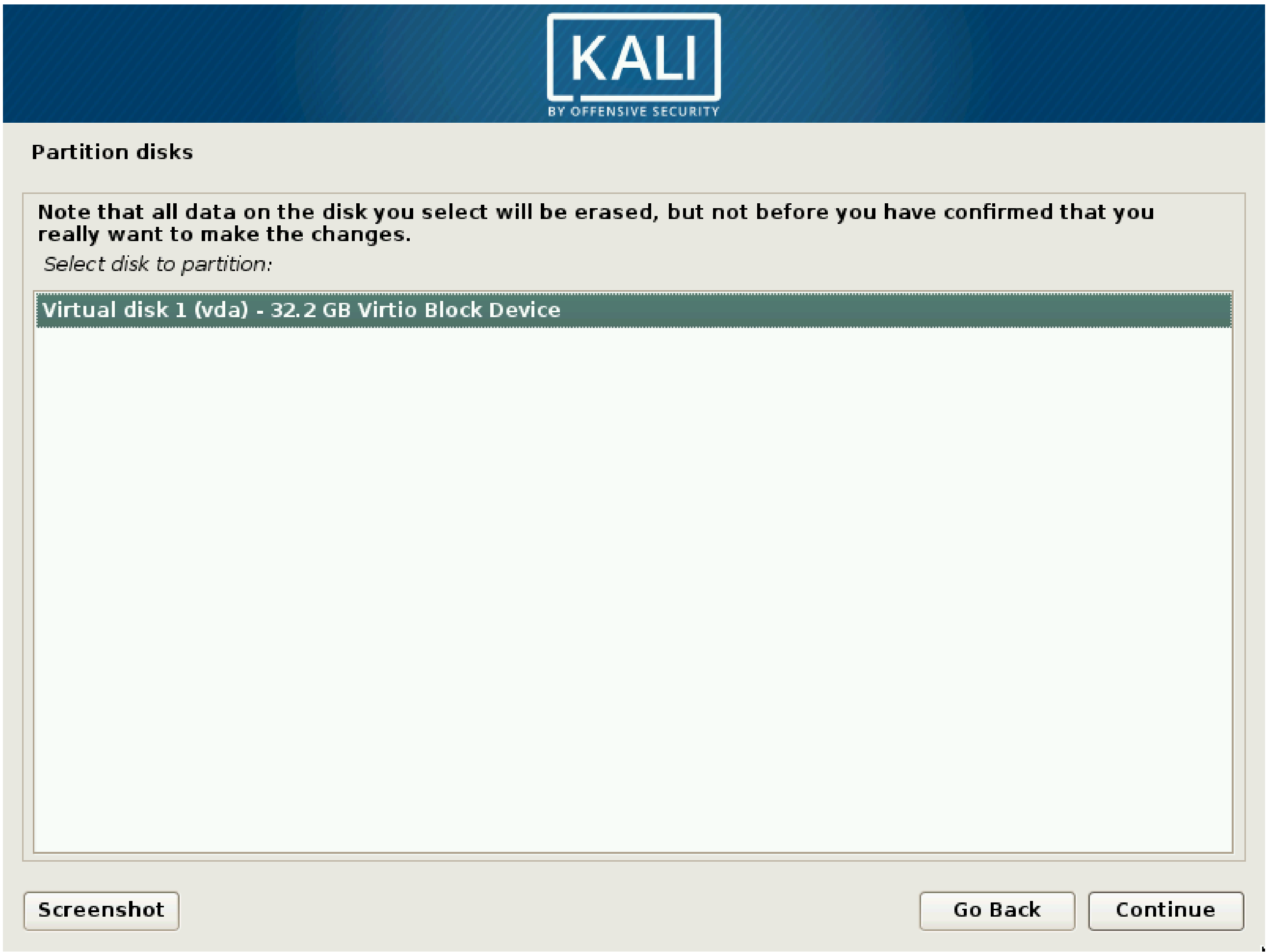
أخيرًا، يبدأ الخيار الأخير في التقسيم اليدوي، والذي يسمح بمزيد من مخططات التقسيم المتقدمة، مثل تثبيت Kali Linux إلى جانب أنظمة التشغيل الأخرى. سنناقش الوضع اليدوي في القسم التالي.

في هذا المثال، سنخصص قرصًا ثابتًا بالكامل لـ Kali، لذلك نختار " Guided – use entire disk " للمتابعة إلى الخطوة التالية.



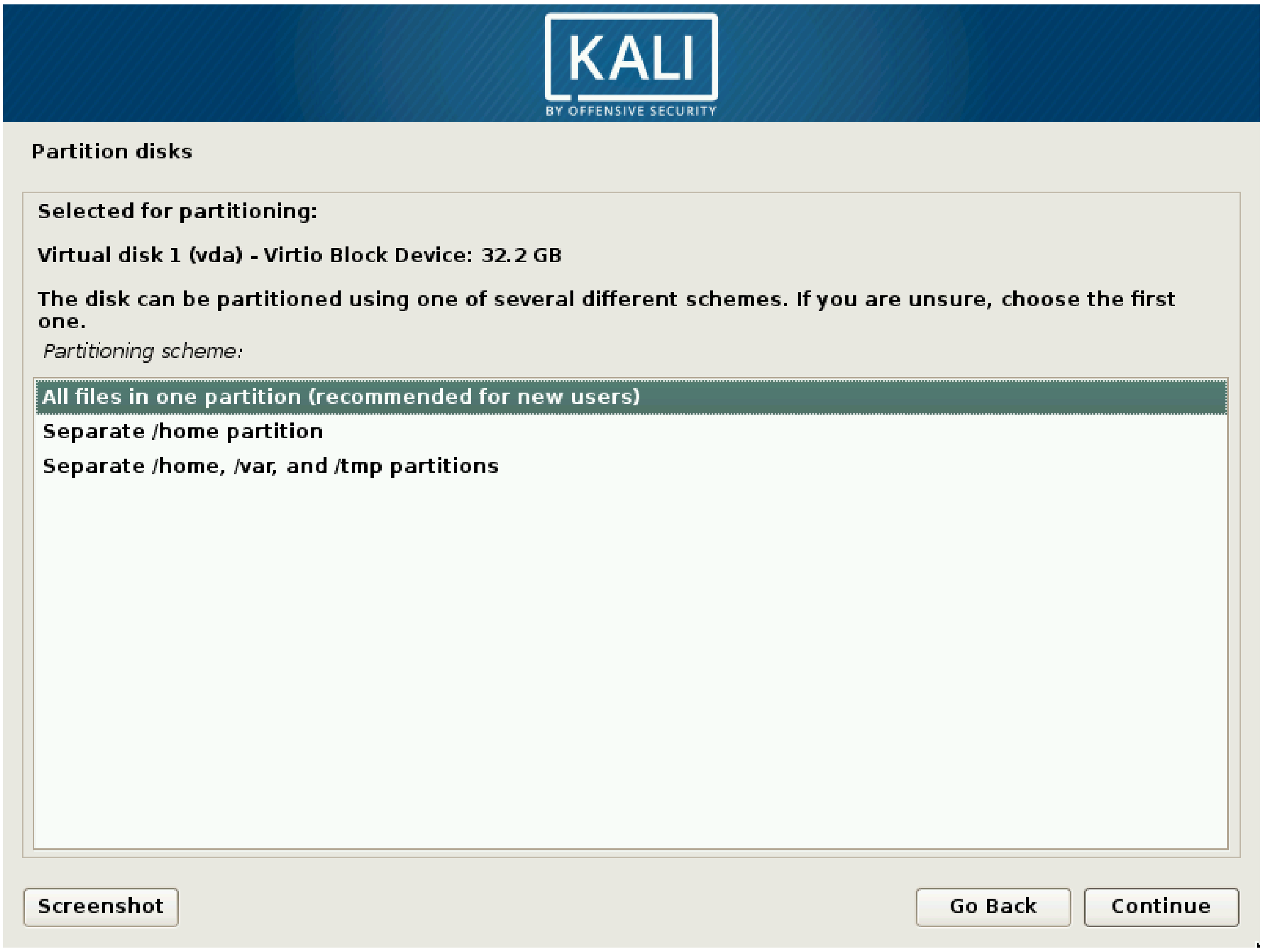
شكل ٨.٤. اختيار وضع التقسيم

تتيح لك الشاشة التالية (الموضحة في الشكل ٩.٤. "القرص المطلوب استخدامه للتقسيم الموجه") اختيار القرص الذي سيتم تثبيت Kali فيه عن طريق تحديد الإدخال المقابل (على سبيل المثال، "Virtual disk 1 (vda) – 32.2 GB Virtio Block Device"). بمجرد تحديده، سيستمر التقسيم الموجه. هذا الخيار سوف يمحو جميع البيانات الموجودة على هذا القرص، لذلك اختر بحكمة.



شكل ٩.٤. القرص المطلوب استخدامه للتقسيم الموجه

بعد ذلك، تقدم أداة التقسيم الموجهة ثلاث طرق تقسيم، والتي تتوافق مع استخدامات مختلفة، كما هو موضح في الشكل ٤.١٠، "تخصيص التقسيم الموجه".



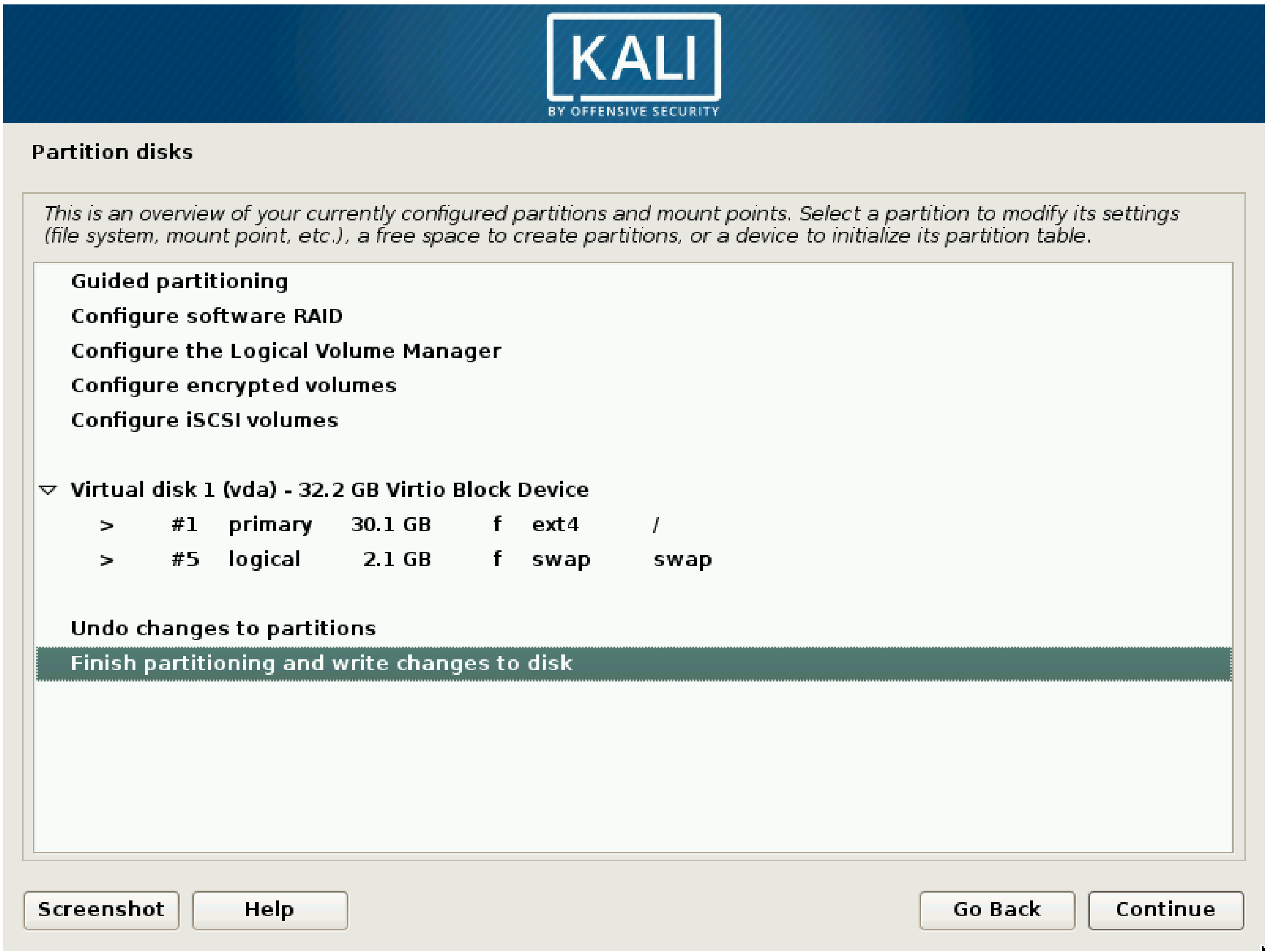
شكل ٤.١٠. تخصيص التقسيم الموجه

تسمى الطريقة الأولى "All files in one partition". يتم تخزين شجرة نظام Linux بالكامل في نظام ملفات واحد، يتوافق مع مجلد الجذر ("/"). يعمل نظام التقسيم البسيط والقوي هذا بشكل جيد على الأنظمة الشخصية أو أنظمة المستخدم المفرد. على الرغم من الاسم، سيتم إنشاء قسمين بالفعل: الأول يضم النظام الكامل، والثاني الذاكرة الافتراضية (أو "المبادلة" "Swap").

تتشابه الطريقة الثانية، "Separate **/home/** partition"، ولكنها تقسم التسلسل الهرمي للملف إلى قسمين: قسم واحد يحتوي على نظام Linux (/)، والثاني يحتوي على "مجلدات home" (بمعنى بيانات المستخدم، في الملفات والمجلدات الفرعية متاح في **/home/**). من بين فوائد هذه الطريقة أنه من السهل الحفاظ على بيانات المستخدمين إذا كان عليك إعادة تثبيت النظام.

إن طريقة التقسيم الأخيرة، والتي تسمى "Separate **/home**, **/var**, and **/tmp** partitions"، مناسبة للخوادم وأنظمة المستخدمين المتعددين. يقسم شجرة الملفات إلى عدة أقسام: بالإضافة إلى أقسام الجذر (/) وحسابات المستخدمين (**/home/**)، كما أنه يحتوي على أقسام لبيانات برنامج الخادم (**/var/**)، والملفات المؤقتة (**/tmp/**). من فوائد هذه الطريقة أنه لا يمكن للمستخدمين قفل الخادم عن طريق استهلاك كل مساحة القرص الصلب المتاحة (يمكنهم فقط ملء **/tmp/** و **/home/**). في الوقت نفسه، لم تعد بيانات البرنامج الخفي (خاصة السجلات) تسد باقي النظام.

بعد اختيار نوع القسم، يقدم المثبت ملخصًا لاختياراتك على الشاشة كخريطة الأقسام (شكل ٤.١١. "التحقق من صحة التقسيم"). يمكنك تعديل كل قسم على حدة عن طريق تحديد قسم، على سبيل المثال: يمكنك اختيار نظام ملفات آخر إذا كان (*ext4*) غير مناسب. ومع ذلك، في معظم الحالات، يكون التقسيم المقترح معقولًا ويمكنك قبوله عن طريق اختيار " Finish partitioning and write changes to disk ". قد يستمر الأمر دون أن يقول ذلك، ولكن اختر بحكمة لأن هذا سيمحو محتويات القرص المحدد.



شكل ٤.١١. التحقق من صحة التقسيم

٢.١٢.١.٢.٤. التقسيم اليدوي

يتيح اختيار Manual في الشاشة الرئيسية "Partition disks" (شكل ٨.٤. "اختيار وضع التقسيم") مرونة أكبر، مما يسمح لك باختيار تكوينات أكثر تقدماً وإملاء غرض وحجم كل قسم على وجه التحديد. على سبيل المثال، يسمح لك هذا الوضع بتثبيت Kali إلى جانب أنظمة التشغيل الأخرى، وتمكين مجموعة متكررة قائمة على البرامج من الأقراص المستقلة " Redundant Array of Independent Disks"(RAID) لحماية البيانات من فشل القرص الصلب، وتغيير حجم الأقسام الموجودة بأمان دون فقدان البيانات، من بين أشياء أخرى.

إذا كنت مستخدمًا أقل خبرة يعمل على نظام يحتوي على بيانات حالية، فيرجى توخي الحذر الشديد مع طريقة الإعداد هذه، لأنه من السهل جدًا ارتكاب أخطاء قد تؤدي إلى فقدان البيانات.

تقليص قسم الوندوز

لتثبيت Kali Linux جنباً إلى جنب مع نظام تشغيل موجود (Windows أو غيره)، ستحتاج إلى مساحة متوفرة على القرص الصلب غير المستخدمة للأقسام المخصصة لـ Kali. في معظم الحالات، يعني هذا تقليص قسم موجود وإعادة استخدام المساحة المحررة.

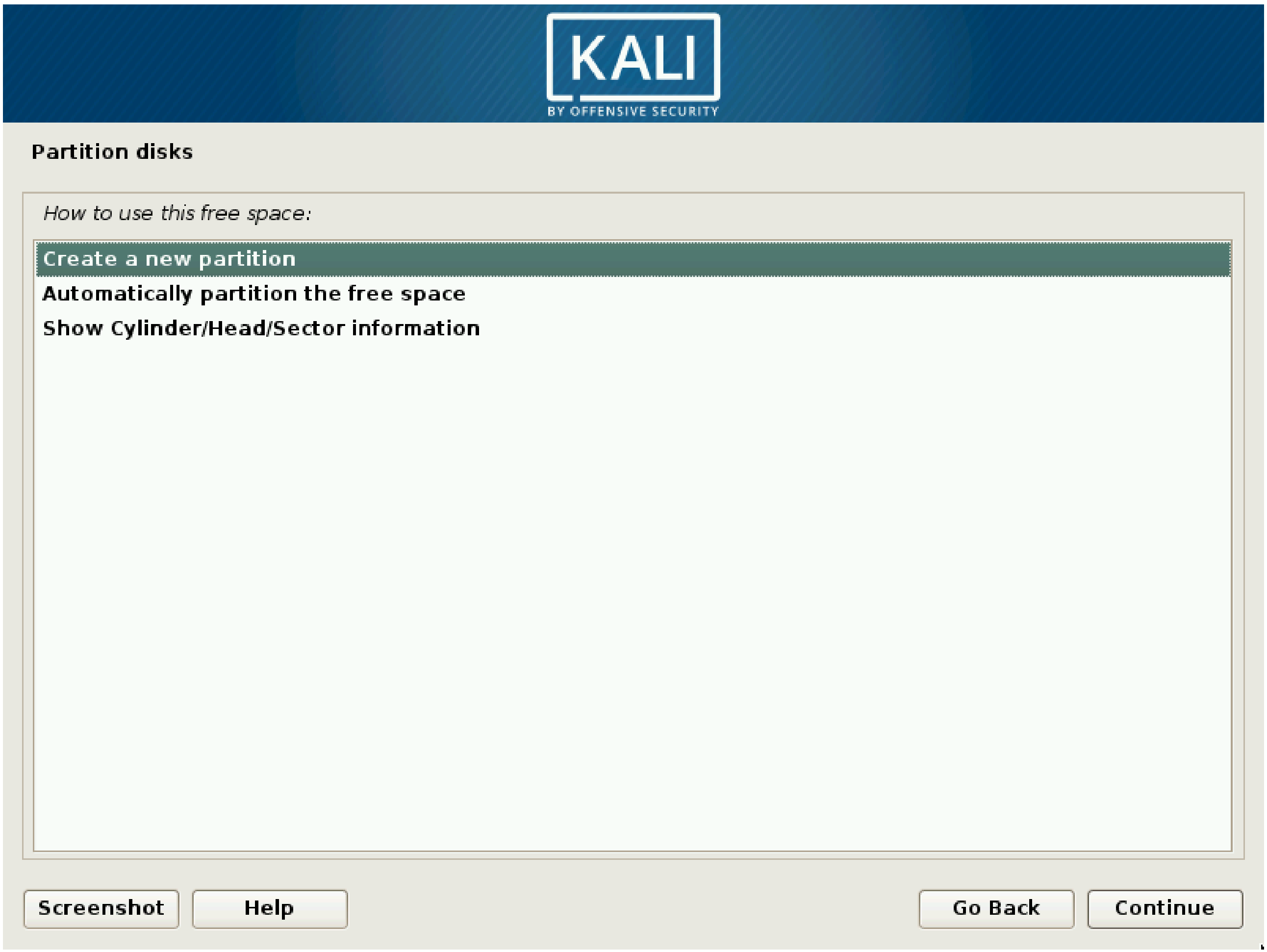
إذا كنت تستخدم وضع التقسيم اليدوي، فيمكن للمثبت تقليص قسم Windows بسهولة تامة. ما عليك سوى اختيار قسم Windows وإدخال حجمه الجديد (يعمل هذا مع كل من أقسام FAT وNTFS).

الشاشة الأولى في برنامج التثبيت اليدوي هي في الواقع نفس الشاشة الموضحة في الشكل ١١.٤. "التحقق من صحة التقسيم" ، باستثناء أنه لا يتضمن أي أقسام جديدة لإنشائها. الأمر متروك لك لإضافة ذلك.

أولاً، سترى خيارًا لإدخال "Guided partitioning" متبوعًا بعدة خيارات تكوين. بعد ذلك، سيعرض برنامج التثبيت الأقراص المتوفرة وأقسامها وأي مساحة حرة ممكنة لم يتم تقسيمها بعد. يمكنك تحديد كل عنصر معروض والضغط على مفتاح **Enter** للتفاعل معه، كالمعتاد.

إذا كان القرص جديد تمامًا، فقد تضطر إلى إنشاء جدول أقسام. يمكنك القيام بذلك عن طريق اختيار القرص. بمجرد الانتهاء من ذلك، سترى مساحة حرة متوفرة داخل القرص.

للاستفادة من هذه المساحة الحرة، يجب عليك تحديدها وسيقدم لك المثبت طريقتين لإنشاء أقسام في تلك المساحة.

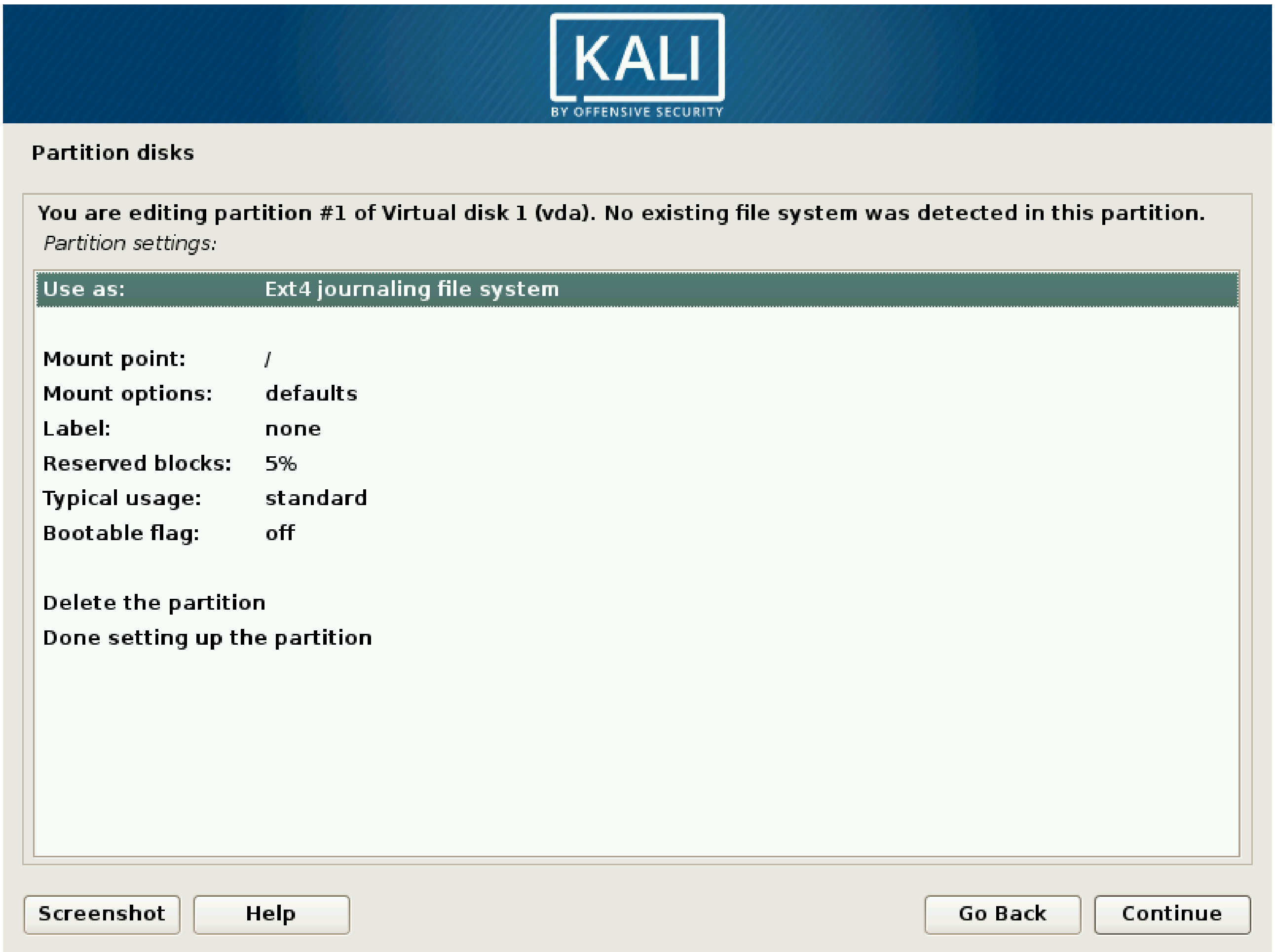


شكل ٤.١٢. إنشاء أقسام في المساحة الحرة

سيقوم الخيار الأول بإنشاء قسم واحد بالخصائص (بما في ذلك الحجم) من اختيارك. سيستخدم الإدخال الثاني كل المساحة الحرة وسيخلق أقسامًا متعددة فيه بمساعدة معالج التقسيم الموجه (انظر القسم ٤.٢.١.١٢.١. "التقسيم الموجه"). يعد هذا الخيار ممتعًا بشكل خاص عندما تريد تثبيت Kali إلى جانب نظام تشغيل آخر ولكن عندما لا ترغب في إدارة تخطيط القسم بشكل دقيق. سيظهر الخيار الأخير أرقام cylinder/head/sector لبداية ونهاية المساحة الحرة.

عندما تختار "Create a new partition"، فسوف تدخل في سلسلة من تسلسل التقسيم اليدوي. بعد تحديد هذا الخيار، ستتم مطالبتك بحجم القسم. إذا كان القرص يستخدم جدول قسم MSDOS، فسيتم إعطاؤك خيار إنشاء قسم أساسي أو منطقي. (أشياء يجب معرفتها: لا يمكن أن

يكون لديك سوى أربعة أقسام أساسية ولكن هناك العديد من الأقسام المنطقية. القسم الذي يحتوي على `boot/`، تتبعه النواة، يجب أن يكون قسمًا أساسيًا، والأقسام المنطقية موجودة في قسم ممتد، يستهلك أحد الأقسام الأربعة الأساسية.) ثم سترى شاشة تكوين القسم العام:



شكل ٤.١٣. شاشة تكوين الأقسام

لتلخيص هذه الخطوة من التقسيم اليدوي، دعونا نلقي نظرة على ما يمكنك القيام به مع القسم الجديد. تستطيع:

❖ تنسيقه وتضمينه في شجرة الملفات عن طريق اختيار نقطة وصل.

نقطة الوصل: هي المجلد الذي سيضم محتويات نظام الملفات على القسم المحدد. وبالتالي، يُقصد عادةً بالقسم المُركب على /**home**/ أن يحتوي على بيانات المستخدم، بينما يُعرف **"/"** باسم جذر شجرة الملفات، وبالتالي فإن قسم الجذر هو الذي سيستضيف نظام `Kali` بالفعل.

❖ استخدامه كقسم المبادلة. عندما تفتقر نواة Linux إلى ذاكرة حرة كافية، فإنها تخزن أجزاء غير نشطة من ذاكرة الوصول العشوائي في قسم تبادل خاص على القرص الثابت. يجعل النظام الفرعي للذاكرة الافتراضية هذا شفافاً للتطبيقات. لمحاكاة الذاكرة الإضافية، يستخدم Windows ملف المبادلة (الترحيل) الموجود مباشرة في نظام الملفات. على العكس من ذلك، يستخدم Linux قسماً مخصصاً لهذا الغرض، ومن هنا يأتي مصطلح قسم التبادل.

❖ جعله "physical volume for encryption" لحماية سرية البيانات على أقسام معينة. تتم أتمتة هذه الحالة في التقسيم الموجه. انظر القسم ٢.٢.٤."التثبيت على نظام ملفات مشفرة بالكامل" لمزيد من المعلومات.

❖ جعله "حجماً فعلياً لـ LVM" (غير مشمول في هذا الكتاب). لاحظ أن هذه الميزة يتم استخدامها بواسطة التقسيم الموجه عند إعداد أقسام مشفرة.

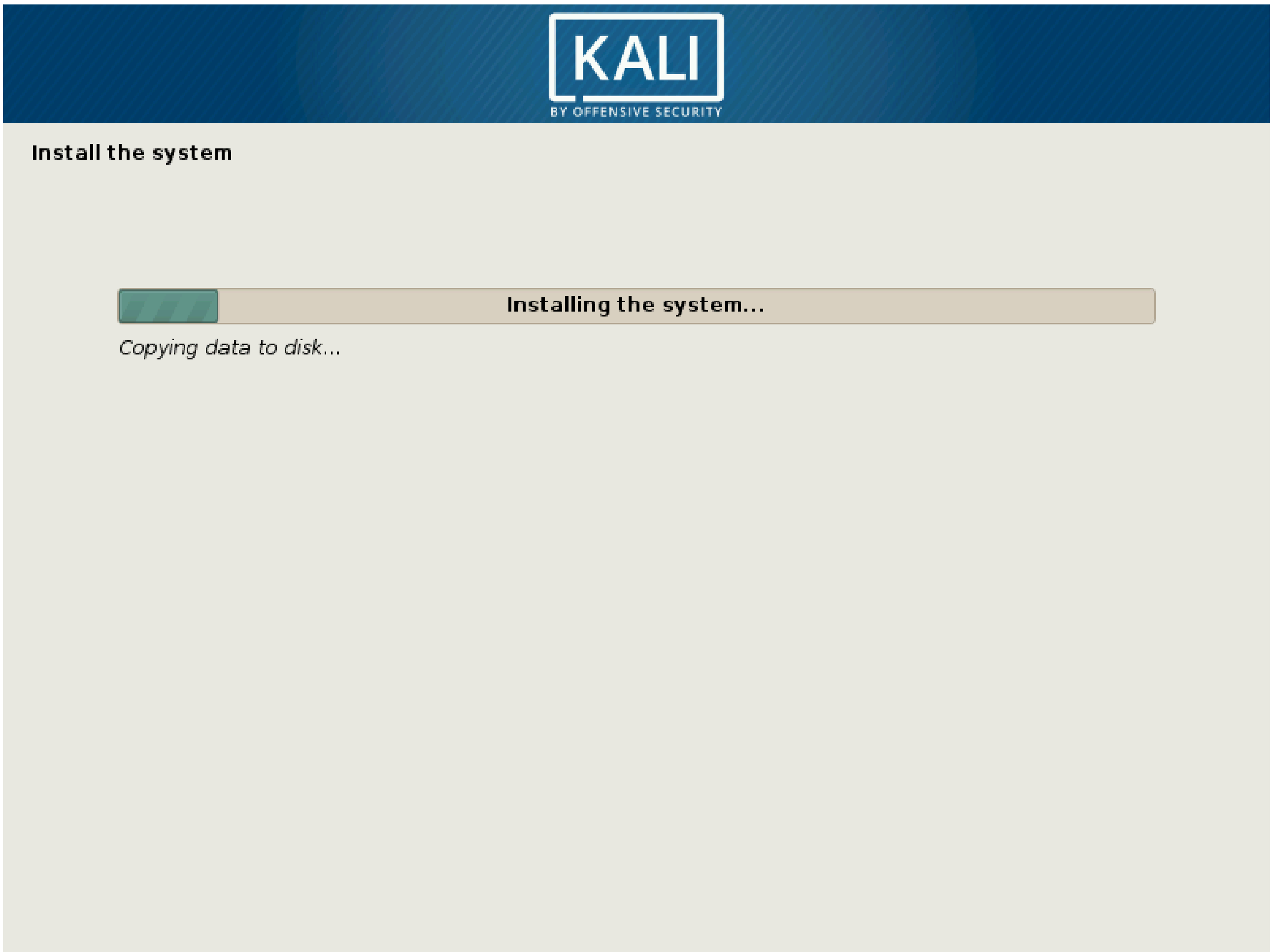
❖ استخدمه كجهاز RAID (غير مشمول في هذا الكتاب).

❖ اختيار عدم استخدام القسم واتركه دون تغيير.

عند الانتهاء، يمكنك إما الرجوع عن التقسيم اليدوي عن طريق اختيار "تراجع عن التغييرات إلى أقسام" أو كتابة التغييرات على القرص عن طريق تحديد "إنهاء التقسيم وكتابة التغييرات على القرص" من شاشة المثبت اليدوي (الشكل ١١.٤. "التحقق من صحة التقسيم").

١٣.١.٢.٤. نسخ الصورة المباشرة

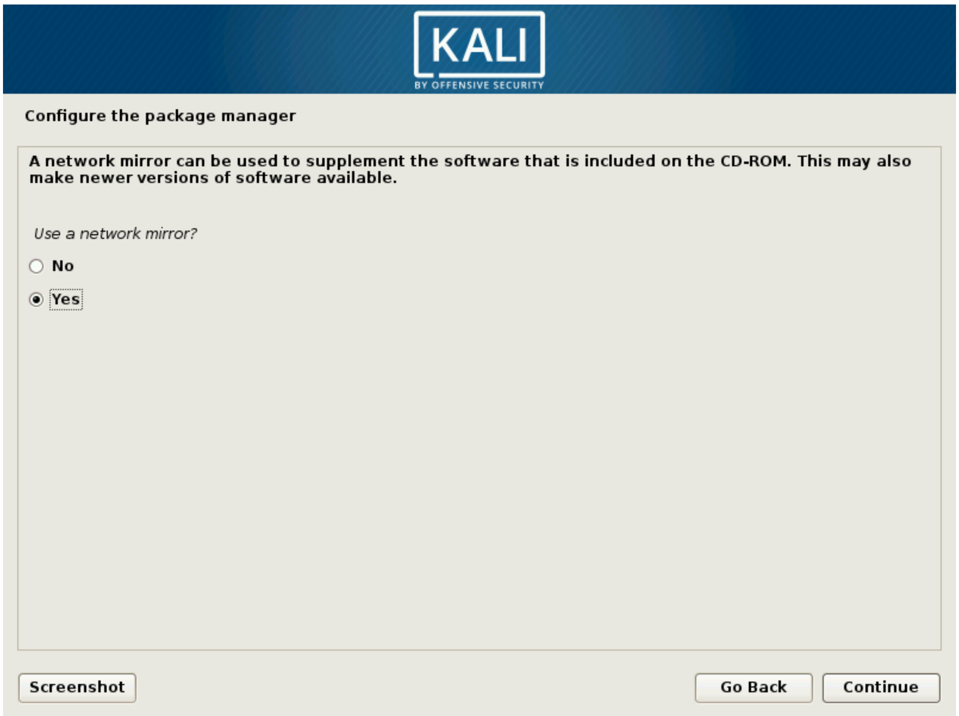
هذه الخطوة التالية، التي لا تتطلب أي تدخل من المستخدم، تنسخ محتويات الصورة المباشرة إلى نظام الملفات الهدف، كما هو موضح في الشكل ١٤.٤. "نسخ البيانات من الصورة المباشرة".



شكل ١٤.٤. نسخ البيانات من الصورة المباشرة

١٤.١.٢.٤. تكوين مدير الحزم (apt)

لكي تكون قادرًا على تثبيت برامج إضافية، يلزم تكوين APT وإخباره عن مكان حزم ديبان. في كالي، هذه الخطوة غير تفاعلية في أغلب الأحيان حيث نجبر المرآة على أن تكون **http.kali.org**. عليك فقط تأكيد ما إذا كنت تريد استخدام هذه النسخة المتطابقة (الشكل ١٥.٤. "استخدام مرآة شبكة؟"). إذا لم تستخدمها، فلن تتمكن من تثبيت حزم إضافية بـ **apt** إلا إذا قمت بتكوين مستودع الحزم لاحقًا.



شكل ١٥.٤. استخدام مرآة الشبكة؟

إذا كنت تريد استخدام نسخة متطابقة محلية بدلاً من **http.kali.org**، يمكنك تمرير اسمها في سطر أوامر النواة (في وقت الإقلاع) باستخدام بناء جملة مثل هذا:

```
mirror/http/hostname=my.own.mirror
```

أخيرًا، يقترح البرنامج استخدام وكيل *HTTP "proxy"* كما هو موضح في الشكل ١٦.٤. "استخدام وكيل HTTP". وكيل HTTP هو خادم يقوم بإعادة توجيه طلبات HTTP لمستخدمي الشبكة.

يساعد في بعض الأحيان على تسريع التنزيلات عن طريق الاحتفاظ بنسخة من الملفات التي تم نقلها من خلالها (ثم نتحدث عن وكيل للتخزين المؤقت). في بعض الحالات، هي الوسيلة الوحيدة للوصول إلى خادم ويب خارجي؛ في مثل هذه الحالات، لن يتمكن المثبت من تنزيل حزم دبيان إلا إذا قمت بملء هذا الحقل بشكل صحيح أثناء التثبيت. إذا لم تقدم عنوانًا وكيلًا، فسيحاول المثبت الاتصال بالإنترنت مباشرةً.



شكل ٤.١٦. استخدام وكيل http

بعد ذلك، سيتم تنزيل ملفي **Packages.xz** و**Sources.xz** تلقائيًا لتحديث قائمة الحزم المعترف بها من قِبل APT.

١٥.١.٢.٤. تثبيت محمل الإقلاع GRUB

محمل الإقلاع هو أول برنامج يتم تشغيله بواسطة BIOS. يقوم هذا البرنامج بتحميل نواة Linux في الذاكرة ثم تنفيذها. يقدم محمل الإقلاع غالبًا قائمة تتيح لك اختيار النواة المراد تحميلها أو نظام التشغيل للإقلاع.

نظراً لتفوقها التقني، فإن GRUB هو مُحمّل الإقلاع الافتراضي الذي تم تثبيته بواسطة Debian: إنه يعمل مع معظم أنظمة الملفات، وبالتالي لا يحتاج إلى تحديث بعد كل تثبيت نواة جديدة؛ لأنه يقرأ التكوين أثناء الإقلاع ويعثر على الموضع الدقيق من النواة الجديدة.

يجب تثبيت GRUB على سجل الإقلاع الرئيسي (MBR) ما لم يكن لديك بالفعل نظام لينكس آخر مثبت يعرف كيفية تشغيل Kali Linux. كما هو موضح في الشكل ١٧.٤. "تثبيت محمل الإقلاع GRUB على القرص الصلب" ، إن تعديل MBR سيجعل أنظمة التشغيل غير المعترف بها والتي تعتمد عليها غير قابلة للإقلاع حتى تقوم بإصلاح تكوين GRUB.



شكل ١٧.٤. تثبيت محمل الإقلاع GRUB على القرص الصلب

في هذه الخطوة (الشكل ١٨.٤ "الجهاز المطلوب تثبيت محمل الإقلاع عليه")، يجب عليك تحديد الجهاز الذي سيتم تثبيت GRUB عليه. يجب أن يكون هذا هو محرك الإقلاع الحالي.



شكل ١٨.٤. الجهاز المطلوب تثبيت محمل الإقلاع عليه

احترس: محمل الإقلاع والإقلاع المزدوج

تكتشف هذه المرحلة من عملية التثبيت أنظمة التشغيل المثبتة بالفعل على الحاسوب وستقوم تلقائياً بإضافة الإدخالات المقابلة في قائمة الإقلاع. ومع ذلك، ليس كل برامج التثبيت تفعل هذا.

على وجه الخصوص، إذا قمت بتثبيت (أو إعادة تثبيت) Windows بعد ذلك، سيتم محو أداة محمل الإقلاع. سيظل نظام Kali موجود على محرك الأقراص الثابت؛ ولكن لن يكون من الممكن الوصول إليه من قائمة الإقلاع. سيكون عليك حينئذٍ بدء برنامج تثبيت Kali باستخدام المعلمة:

```
rescue/enable=true
```

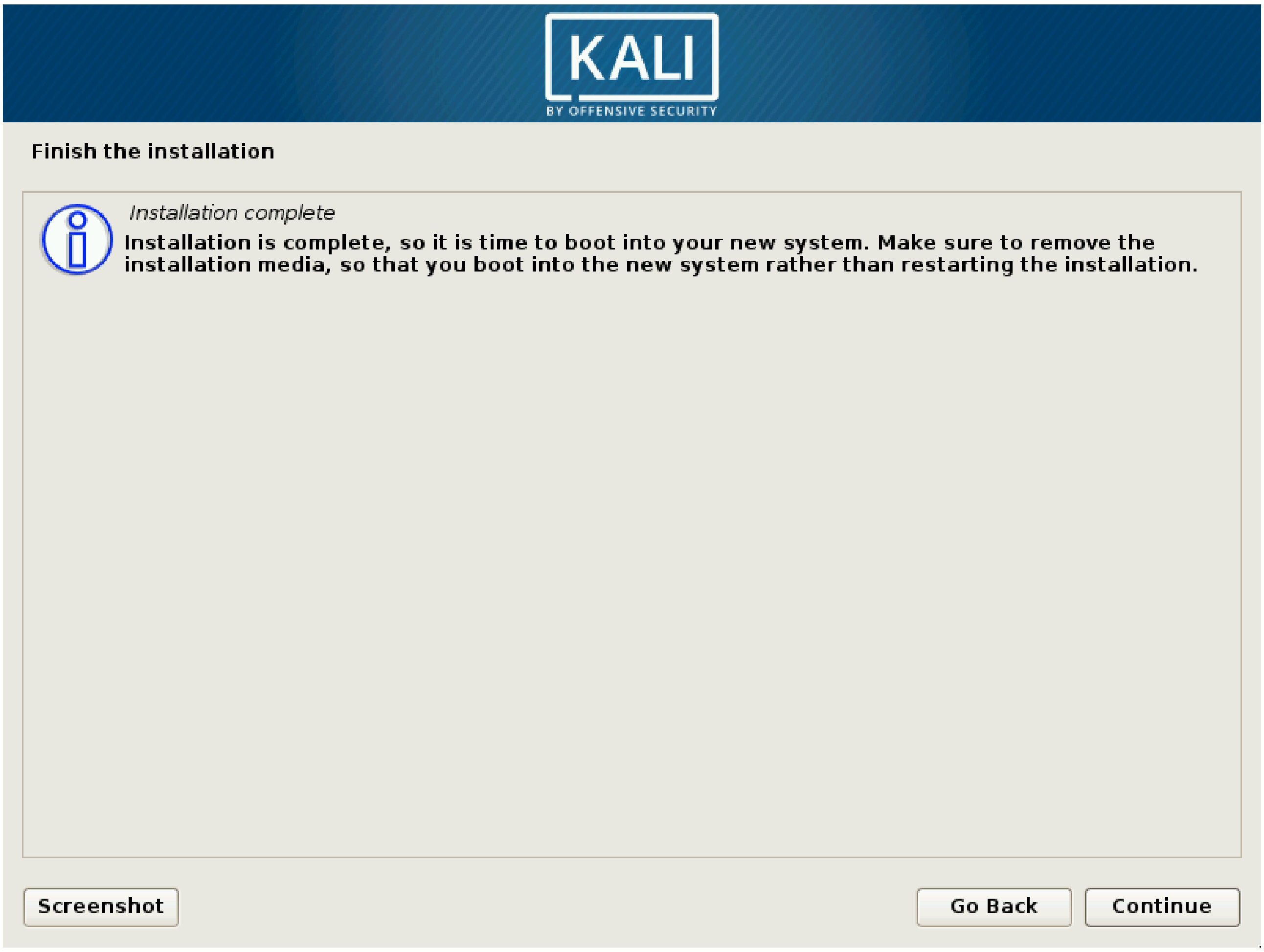
في سطر أوامر النواة لإعادة تثبيت أداة محمل الإقلاع. تم وصف هذه العملية بالتفصيل في دليل تثبيت ديبان.

http://www.debian.org/releases/stable/amd64/ch08s07.html

١٦.١.٢.٤. الانتهاء من التثبيت وإعادة التشغيل

الآن وبعد اكتمال التثبيت، يطلب منك البرنامج إزالة قرص DVD-ROM من القارئ (أو فصل محرك USB الخاص بك) حتى يتمكن جهاز الحاسوب من الإقلاع بنظام Kali الجديد الخاص بك بعد إعادة تشغيل برنامج التثبيت (الشكل ١٩.٤. "اكتمل التثبيت").

أخيراً، سيقوم المثبت ببعض أعمال التنظيف، مثل إزالة الحزم الخاصة بإنشاء البيئة المباشرة.



شكل ١٩.٤. اكتمل التثبيت

٢.٢.٤. التثبيت بنظام ملفات مشفر بالكامل

لضمان سرية بياناتك، يمكنك إعداد أقسام مشفرة. سيؤدي ذلك إلى حماية بياناتك في حالة فقد الحاسوب المحمول أو القرص الصلب أو سرقته. يمكن لأداة التقسيم مساعدتك في هذه العملية، سواء في الوضع الإرشادي أو اليدوي.

سيجمع وضع التقسيم الموجه بين استخدام تقنيتين:

لتشفير الأقسام Linux Unified Key Setup (LUKS)

لإدارة التخزين بشكل حيوي Logical Volume Management (LVM)

يمكن أيضًا ضبط كلتا الميزتين وتكوينهما من خلال وضع التقسيم اليدوي.

١.٢.٢.٤. مقدمة في LVM

دعونا نناقش LVM أولاً. باستخدام مصطلحات LVM، القسم الظاهري هو وحدة تخزين منطقية، والتي تعد جزءًا من مجموعة وحدات تخزين أو مجموعة من عدة وحدات تخزين فعلية. وحدات التخزين الفعلية هي أقسام حقيقية (أو أقسام افتراضية يتم تصديرها بواسطة أدوات تجريدية أخرى، مثل جهاز RAID للبرنامج أو قسم مشفر).

بفضل الافتقار إلى التمييز بين الأقسام "المادية" و "المنطقية"، يتيح لك LVM إنشاء أقسام "افتراضية" تمتد على عدة أقراص. الفوائد ذات شقين: لم يعد حجم الأقسام محددًا من قِبل الأقراص الفردية ولكن بواسطة حجمها التراكمي، ويمكنك تغيير حجم الأقسام الموجودة في أي وقت، مثل بعد إضافة قرص إضافي.

تعمل هذه التقنية بطريقة بسيطة للغاية: يتم تقسيم كل وحدة تخزين، سواء كانت مادية أو منطقية، إلى كتل من نفس الحجم، والتي يرتبط بها LVM. تؤدي إضافة قرص جديد إلى إنشاء وحدة

تخزين فعلية جديدة توفر كمًّا جديدة يمكن ربطها بأي مجموعة وحدات تخزين. يمكن لجميع الأقسام الموجودة في مجموعة مستوى الصوت الاستفادة الكاملة من المساحة المخصصة الإضافية.

٢.٢.٢.٤. مقدمة إلى LUKS

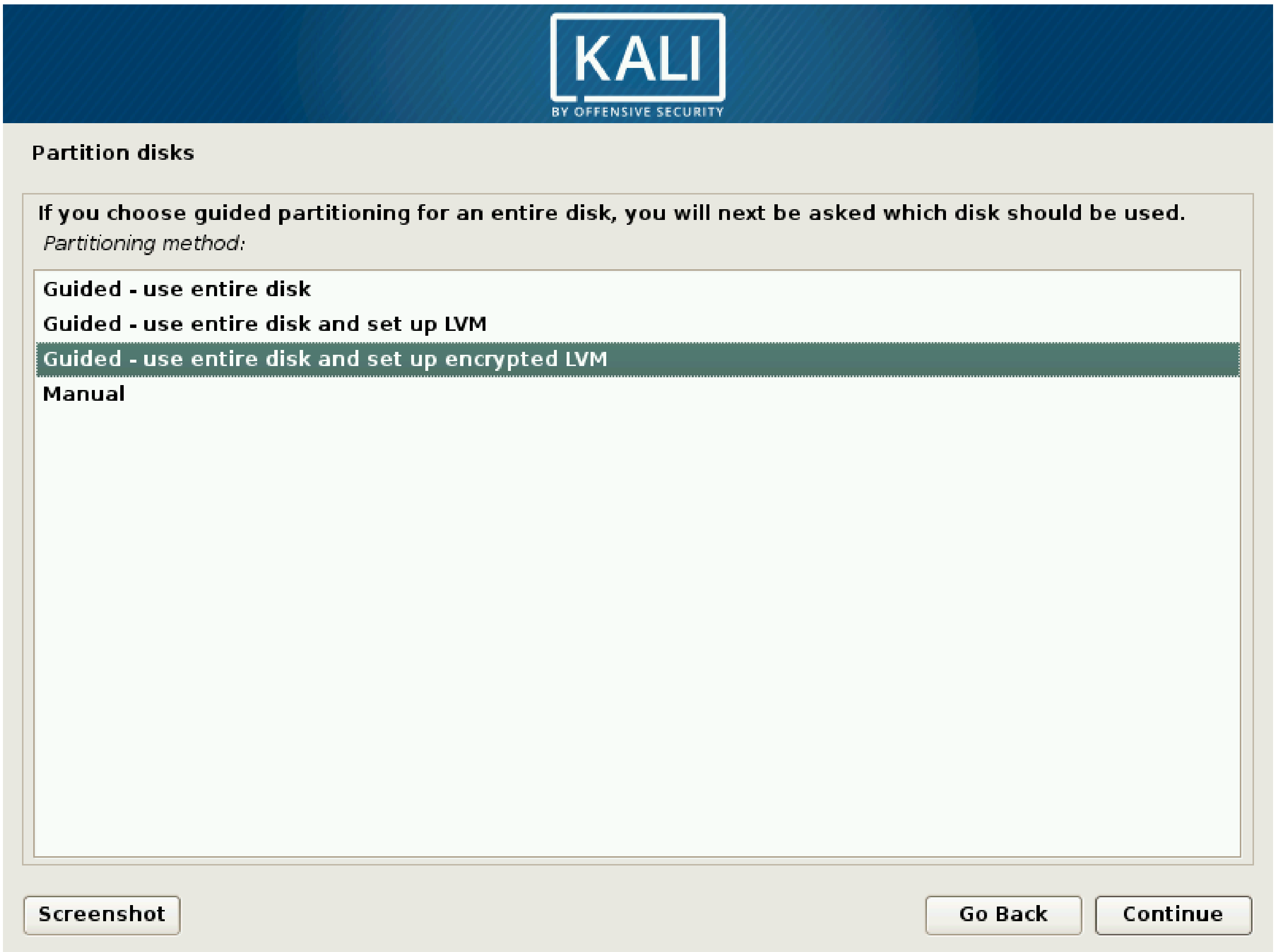
لحماية بياناتك، يمكنك إضافة طبقة تشفير أسفل نظام الملفات الذي تختاره. يستخدم Linux (وخاصة برنامج تشغيل `dm-crypt` معين الجهاز لإنشاء القسم الافتراضي (الذي تكون محتوياته محمية) استنادًا إلى قسم أساسي يقوم بتخزين البيانات في نموذج مشفر (بفضل LUKS). يقيس LUKS تخزين البيانات المشفرة وكذلك معلومات التعريف التي تشير إلى خوارزميات التشفير المستخدمة.

تشفير قسم المبادلة

> عند استخدام قسم مشفر، يتم تخزين مفتاح التشفير في الذاكرة (RAM)، وعند الإسبات، يقوم الحاسوب المحمول بنسخ المفتاح، إلى جانب محتويات أخرى من ذاكرة الوصول العشوائي، إلى قسم المبادلة للقرص الثابت. نظرًا لأن أي شخص لديه حق الوصول إلى ملف المبادلة (بما في ذلك فني أو لص) يمكنه استخراج المفتاح وفك تشفير بياناتك، فيجب حماية ملف المبادلة بالتشفير.
> ولهذا السبب، سوف يحذرك برنامج التثبيت إذا حاولت استخدام قسم مشفر إلى جانب قسم تبديل غير مشفر. في سطر أوامر النواة لإعادة تثبيت أداة محمل الإقلاع. تم وصف هذه العملية بالتفصيل في دليل تثبيت ديبان.
>
> http://www.debian.org/releases/stable/amd64/ch08s07.html

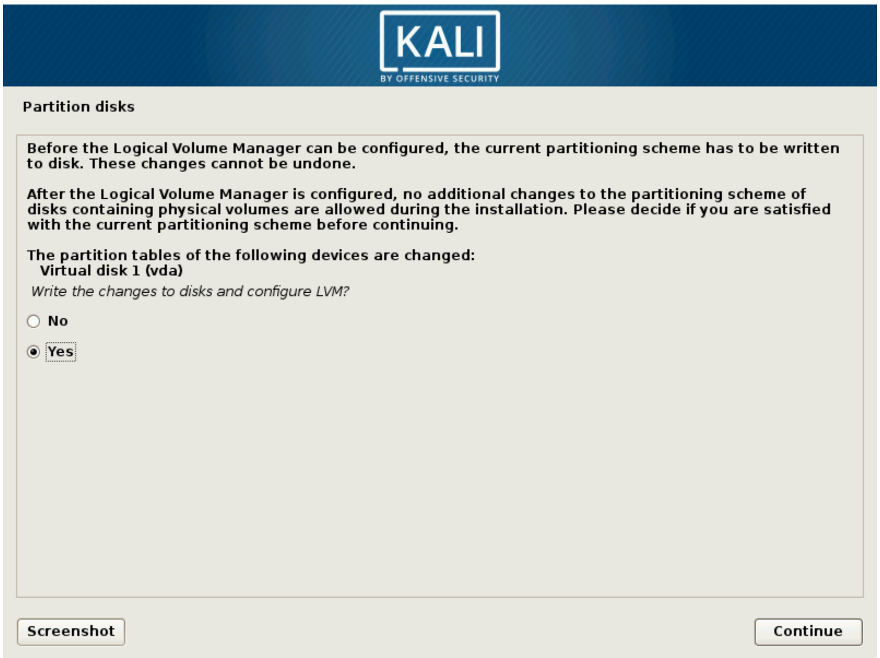
٣.٢.٢.٤. إعداد أقسام مشفرة

إن عملية تثبيت LVM المشفرة هي نفس عملية التثبيت القياسية باستثناء خطوة التقسيم (الشكل ٢٠.٤ "Guided Partitioning with Encrypted LVM") حيث ستختار بدلاً من ذلك "Guided – use entire disk and set up encrypted LVM". ستكون النتيجة نظامًا لا يمكن إقلاعه أو الوصول إليه حتى يتم توفير كلمة مرور التشفير. سيؤدي ذلك إلى تشفير وحماية البيانات الموجودة على القرص.



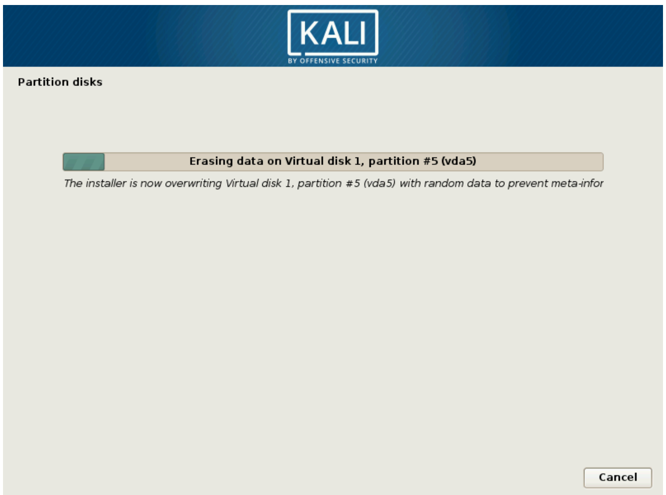
شكل ٢٠.٤. Guided Partitioning with Encrypted LVM

سيقوم مُثبّت التقسيم الموجه تلقائيًا بتعيين قسم فعلي لتخزين البيانات المشفرة، كما هو موضح في الشكل ٢١.٤ "تأكيد التغييرات على جدول الأقسام". في هذه المرحلة، سيقوم المثبت بتأكيد التغييرات قبل كتابتها على القرص.



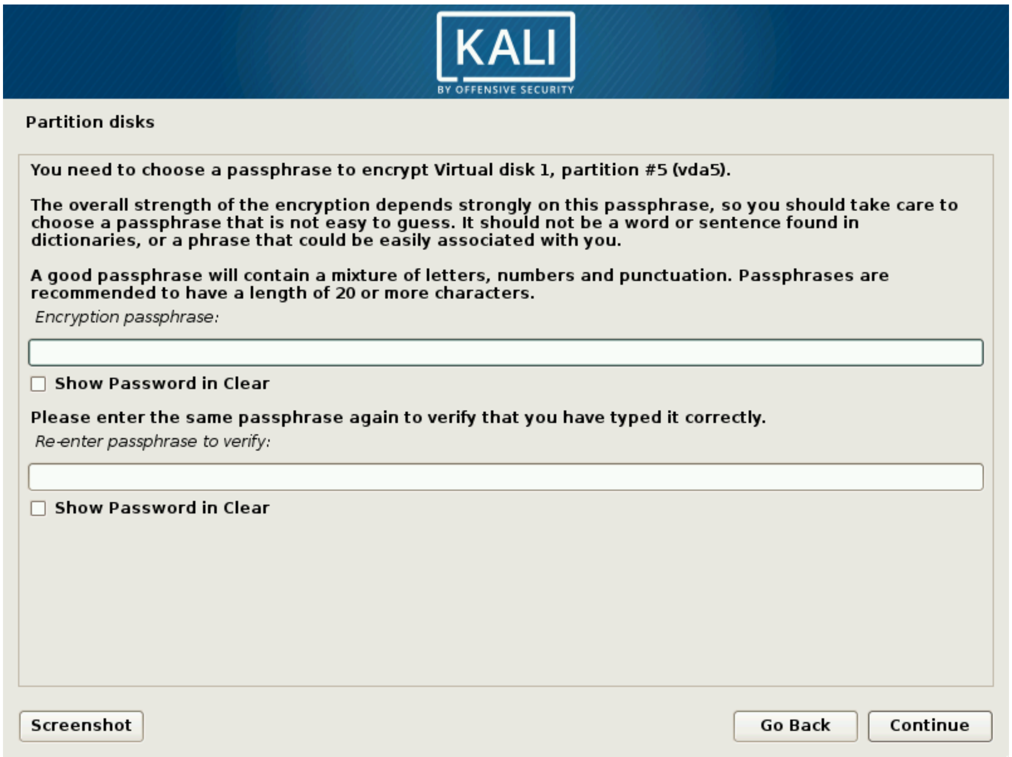
شكل ٢١.٤. تأكيد التغييرات على جدول الأقسام

ثم يتم تهيئة هذا القسم الجديد ببيانات عشوائية، كما هو موضح في الشكل ٢٢.٤. "محو البيانات على القسم المشفر". هذا يجعل المناطق التي تحتوي على بيانات لا يمكن تمييزها عن المناطق غير المستخدمة، مما يجعل من الصعب اكتشاف البيانات المشفرة، ومن ثم مهاجمتها.



الشكل ٢٢.٤. محو البيانات على القسم المشفر

بعد ذلك، يطلب منك برنامج التثبيت إدخال كلمة مرور فك التشفير (الشكل ٢٣.٤."أدخل كلمة مرور فك التشفير"). لعرض محتويات القسم المشفر، ستحتاج إلى إدخال كلمة المرور هذه في كل مرة تقوم فيها بإعادة تشغيل النظام. لاحظ التحذير الموجود في برنامج التثبيت: سيكون نظامك المشفر قويًا بقدر قوة كلمة المرور هذه.

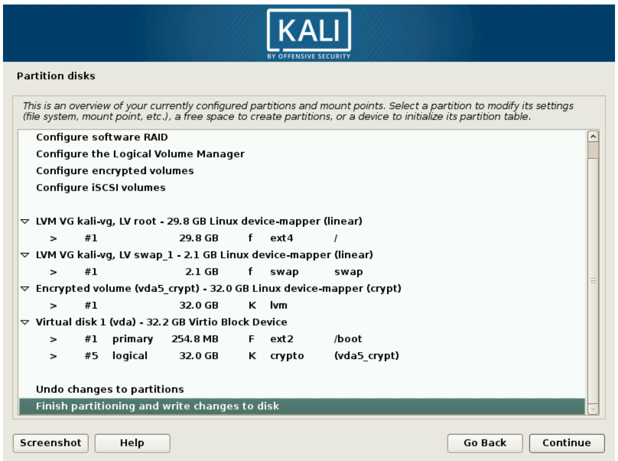


شكل ٢٣.٤. ادخل كلمة مرور التشفير

تمتع أداة التقسيم الآن بالوصول إلى قسم افتراضي جديد يتم تخزين محتوياته مشفرة في القسم الفعلي الأساسي. نظرًا لأن LVM يستخدم هذا القسم الجديد كوحدة تخزين فعلية، يمكنه حماية عدة أقسام (أو وحدات تخزين منطقية LVM) باستخدام مفتاح التشفير نفسه، بما في ذلك قسم المبادلة (انظر الشريط الجانبي Encrypted Swap Partition). هنا، لا يتم استخدام LVM لتسهيل توسيع حجم التخزين، ولكن فقط من أجل توفير الراحة غير المباشرة التي تسمح بتقسيم قسم مشفر واحد إلى وحدات تخزين منطقية متعددة.

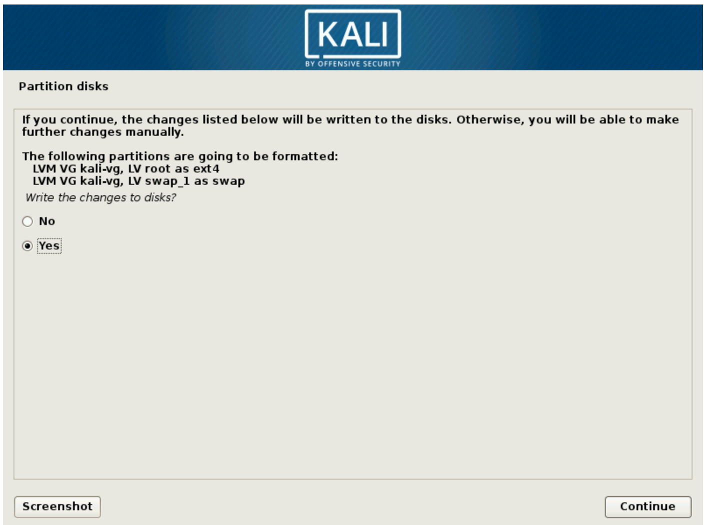
٤.٢.٢.٤. نهاية التقسيم الموجه باستخدام LVM المشفر

بعد ذلك، يتم عرض مخطط التقسيم الناتج (الشكل ٢٤.٤. "التحقق من صحة التقسيم لتثبيت LVM المشفر") حتى تتمكن من تعديل الإعدادات حسب الحاجة.



شكل ٢٤.٤. التحقق من صحة التقسيم لتثبيت LVM المشفر

أخيرًا، بعد التحقق من صحة إعداد القسم، تطلب الأداة تأكيد كتابة التغييرات على الأقراص، كما هو موضح في الشكل ٢٥.٤. "تأكيد الأقسام المراد تنسيقها".



شكل ٢٥.٤. تأكيد الأقسام المراد تنسيقها

أخيرًا، تستمر عملية التثبيت كالمعتاد كما هو موضح في القسم ١٤.١.٢.٤. "تكوين مدير الحزم (`apt`)".

٣.٤. التثبيت الغير مراقب

يعد مثبّتا ديبان وكالي نمطياً للغاية: على المستوى الأساسي، ينفّذان فقط العديد من البرامج النصية (محزومة في حزم صغيرة تسمى udeb — لـ µdeb أو micro-deb) واحدة تلو الأخرى. يعتمد كل برنامج نصي على debconf (راجع أداة debconf)، التي تتفاعل معك والمستخدم وتخزين معلمات التثبيت. لهذا السبب، يمكن أيضًا تثبيت برنامج التثبيت تلقائيًا من خلال أتمتة debconf preseeding، وهي دالة تتيح لك تقديم إجابات غير مراقبة لأسئلة التثبيت.

١.٣.٤. الإجابات المعدة مسبقا

هناك طرق متعددة لاستباق الإجابات على المثبت. كل أسلوب له مزاياه وعيوبه. بناءً على وقت حدوث عملية التغذية السابقة، تختلف الأسئلة التي يمكن إجراؤها.

١.١.٣.٤. مع معلمات الإقلاع

يمكنك أن تسبق أي سؤال مثبّت مع معلمات الإقلاع تنتهي في سطر أوامر النواة، يمكن الوصول إليها من خلال proc/cmdline/. ستتيح لك بعض أدوات تحميل الإقلاع تحرير هذه المعلمات بشكل تفاعلي (وهو أمر عملي لأغراض الاختبار)، ولكن إذا كنت تريد إجراء التغييرات، فسيتعين عليك تعديل تكوين أداة تحميل الإقلاع.

يمكنك استخدام المعرف الكامل لأسئلة debconf مباشرةً (مثل debian-installer/language=en) أو يمكنك استخدام الاختصارات للأسئلة الأكثر شيوعًا (مثل language=en أو hostname=duke). انظر القائمة الكاملة للأسماء المستعارة –aliases- في دليل تثبيت ديبان.

لا يوجد أي قيود على الأسئلة التي يمكنك إجراؤها لأن معلمات الإقلاع متوفرة من بداية عملية التثبيت وتتم معالجتها في وقت مبكر جدًا. ومع ذلك، يقتصر عدد معلمات الإقلاع على 32 وعددًا من تلك المعلمات يتم استخدامها بالفعل افتراضيًا. من المهم أيضًا إدراك أن تغيير تكوين محمل الإقلاع يمكن أن يكون غير تافه في بعض الأحيان.

في القسم ٣.٩، "Building Custom Kali Live ISO Images"، ستتعلم أيضًا كيفية تعديل تكوين Isolinux عند إنشاء صورة Kali ISO الخاصة بك.

٢.١.٣.٤. مع ملف preseed في البداية

يمكنك إضافة ملف باسم preseed.cfg في جذر initrd الخاص بالمثبت (هذا هو initrd الذي يُستخدم لبدء المثبت). عادةً ما يتطلب ذلك إعادة إنشاء حزمة مصدر debian-installer لإنشاء إصدارات جديدة من initrd. ومع ذلك، يوفر التصميم المباشر طريقة مناسبة للقيام بذلك، وهو موضح بالتفصيل في القسم ٣.٩، "صور مخصصة بناء Kali Live ISO".

لا تحتوي هذه الطريقة أيضًا على أية قيود على الأسئلة التي يمكنك إجراؤها نظرًا لأن ملف preseed متاح فور بدء التشغيل. في كالي، استفدنا بالفعل من هذه الميزة لتخصيص سلوك مثبت دبيان الرسمي.

٣.١.٣.٤. مع ملف Preseed في Boot Media

يمكنك إضافة ملف مسبق على وسائط الإقلاع (CD أو مفتاح USB)؛ يحدث ذلك قبل بدء الوسائط، مما يعني مباشرة بعد الأسئلة حول تخطيط اللغة ولوحة المفاتيح. يمكن استخدام المعلمة الإقلاع preseed/file للإشارة إلى موقع ملف preseed (على سبيل المثال، cdrom/preseed.cfg/ عند التثبيت من قرص مضغوط أو hd-media/preseed.cfg/ عند التثبيت من مفتاح USB).

لا يجوز لك تقديم إجابات على خيارات اللغة والبلد حيث يتم تحميل ملف preseeding لاحقًا في العملية، بمجرد تحميل برامج تشغيل الأجهزة. على الجانب الإيجابي، تجعل عملية الإنشاء المباشر من السهل وضع ملف إضافي في صور ISO التي تم إنشاؤها (انظر القسم ٩,٣، "صور المباني المخصصة لـ Kali Live ISO").

٤.١.٣.٤. بملف preseed محملة من الشبكة

يمكنك إتاحة ملف مسبق على الشبكة من خلال خادم ويب وإخبار المثبت بتنزيل هذا الملف قبل إضافة معلمة الإقلاع:

preseed/url=http: //server/preseed.cfg (أو باستخدام عنوان url المستعار "alias").

ومع ذلك، عند استخدام هذه الطريقة، تذكر أنه يجب تكوين الشبكة أولاً. هذا يعني أن أسئلة debconf المتعلقة بالشبكة (خاصة اسم المضيف واسم المجال) وجميع الأسئلة السابقة (مثل اللغة

والبلد) لا يمكن إعطاؤها بهذه الطريقة. غالبًا ما يتم استخدام هذه الطريقة مع معلمات الإقلاع التي تسبق هذه الأسئلة المحددة.

طريقة التجميع هذه هي الأكثر مرونة حيث يمكنك تغيير تكوين التثبيت دون تغيير وسائط التثبيت.

تأخير أسئلة اللغة، البلد، لوحة المفاتيح

> للتغلب على قيود عدم القدرة على الافتراض على أسئلة اللغة والدولة ولوحة المفاتيح، يمكنك إضافة معلمة الإقلاع `auto-install/enable=true` (أو `auto = true`). باستخدام هذا الخيار، سيتم طرح الأسئلة لاحقًا في هذه العملية، بعد تهيئة الشبكة، وبالتالي بعد تنزيل الملف الرئيسي.
> الجانب السلبي هو أن الخطوات الأولى (لا سيما تكوين الشبكة) ستحدث دائمًا باللغة الإنجليزية، وإذا كانت هناك أخطاء، فسيتعين على المستخدم العمل من خلال شاشات باللغة الإنجليزية (مع تكوين لوحة مفاتيح في(QWERTY).

4.3.2. إنشاء ملفpreseed

ملف preseed هو ملف نصي عادي يحتوي فيه كل سطر على إجابة لسؤال Debconf واحد. يتم تقسيم السطر عبر أربعة حقول مفصولة بمسافة بيضاء (مسافات أو علامات تبويب). على سبيل المثال، d-i mirror/suite string kali-rolling:

يشير الحقل الأول إلى صاحب السؤال. على سبيل المثال، يتم استخدام "d-i" للأسئلة ذات الصلة المثبت. قد ترى أيضًا اسم الحزمة، للأسئلة الواردة من حزم دبيان (كما في هذا المثال: atftpd atftpd/use_inetd boolean false).

الحقل الثاني هو معرف للسؤال.

يسرد الحقل الثالث نوع السؤال.

يحتوي الحقل الرابع والأخير على قيمة الإجابة المتوقعة. لاحظ أنه يجب فصله عن الحقل الثالث بمسافة واحدة؛ تعتبر أحرف المسافة الإضافية جزءًا من القيمة.

إن أبسط طريقة لكتابة ملف مسبق هي تثبيت النظام يدويا. بعد ذلك، يوفر الأمر debconf-get-selections --installer الإجابات التي قدمتها إلى المثبت. يمكنك الحصول على إجابات موجهة إلى الحزم الأخرى باستخدام debconf-get-selections. ومع ذلك، فإن الحل الأنظف هو كتابة الملف يدويًا، بدءًا من مثال ثم الانتقال إلى الوثائق. باستخدام هذا النهج، يمكن فقط طرح الأسئلة التي تحتاج إلى إبطال الإجابة الافتراضية. قدم الأولوية = معلمة الإقلاع الحرجة لتوجيه Debconf لطرح الأسئلة الهامة فقط، واستخدام الإجابة الافتراضية للآخرين.

٢.٣.٤. إنشاء ملف preseed

ملف preseed هو ملف نصي عادي يحتوي فيه كل سطر على إجابة سؤال Debconf واحد. يتم تقسيم السطر لأربعة حقول مفصولة بمسافة بيضاء (مسافات أو tabs). على سبيل المثال،

```
d-i mirror/suite string kali-rolling:
```

- ❖ يشير الحقل الأول إلى صاحب السؤال. على سبيل المثال، يتم استخدام "d-i" للأسئلة المتعلقة بالمثبت (installer) {{ ولعلها اختصار لـ "debian installer"}}. قد ترى أيضًا اسم حزمة للأسئلة الواردة من حزم دبيان (كما في هذا المثال: / atftpd atftpd use_inetd boolean false).
- ❖ الحقل الثاني هو معرف للسؤال.
- ❖ يسرد الحقل الثالث نوع السؤال.
- ❖ يحتوي الحقل الرابع والأخير على قيمة الإجابة المتوقعة. لاحظ أنه يجب فصله عن الحقل الثالث بمسافة واحدة؛ تعتبر أحرف المسافات الإضافية جزءًا من القيمة.

إن أبسط طريقة لكتابة ملف preseed هي تثبيت النظام يدويًا. ثم سيقدم الأمر:

```
debconf-get-selections - installer
```

الإجابات التي قدمتها للمثبت. يمكنك الحصول على إجابات موجهة إلى الحزم الأخرى باستخدام:

```
debconf-get-selections
```

ومع ذلك، فإن الحل الأنظف هو كتابة الملف يدويًا، بدءًا من المثال ثم المرور بالوثائق. باستخدام هذا النهج، يمكن فقط توقع الأسئلة التي تحتاج إلى تجاوز الإجابة الافتراضية. قدّم معلمة الإقلاع:

```
priority=critical
```

لـ (مرشد ديبيان) Instruct Debconf إلى طرح الأسئلة المهمة فقط، واستخدام الإجابة الافتراضية لغير ذلك.

ملحق دليل التثبيت

يحتوي دليل تثبيت دبيان، المتاح عبر الإنترنت، على وثائق تفصيلية حول استخدام ملف preseed في الملحق. كما يشمل أيضا ملف مفصل وتعليقات بسيطة، يمكن أن يكون بمثابة قاعدة للتخصيصات المحلية.

https://www.debian.org/releases/stable/amd64/apb.html

https://www.debian.org/releases/stable/example-preseed.txt

لاحظ أن الروابط السابقة توثق الإصدار المستقر من دبيان وأن كالي يستخدم الإصدار التجريبي (Debian testing)، لذا فقد تواجه اختلافات بسيطة. يمكنك أيضًا الرجوع إلى دليل التثبيت المستضاف على موقع مشروع مثبت ديبيان (Debian-installer). قد يكون أكثر حداثة.

٤.٤. تثبيت على أجهزة ARM

يعمل Kali Linux على مجموعة متنوعة من الأجهزة المستندة إلى ARM (أجهزة الحاسوب المحمولة وأجهزة الحاسوب المضمنة ولوحات المطورين، على سبيل المثال) ولكن لا يمكنك استخدام مثبت Kali التقليدي على هذه الأجهزة نظرًا لأنها غالبًا ما تكون لها متطلبات محددة فيما يتعلق بتكوين النواة أو محمل الإقلاع.

لجعل هذه الأجهزة في متناول مستخدمي Kali، قامت Offensive Security بتطوير نصوص برمجية لإنشاء صور قرص جاهزة للاستخدام لأجهزة ARM المختلفة. توفر هذه الصور للتنزيل على موقعها على الويب:

https://www.offensive-security.com/kali-linux-arm-images/

نظرًا لأن هذه الصور متاحة، فإن مهمتك في تثبيت Kali على جهاز ARM بسيطة لحد كبير. وهنا الخطوات الأساسية:

❖ قم بتنزيل الصورة لجهاز ARM الخاص بك وتأكد من أن المجموع الاختباري يطابق الموجود على موقع الويب (انظر القسم ٣.١.٢، "التحقق من النزاهة والأصالة" للحصول على توضيحات حول كيفية القيام بذلك). لاحظ أن الصور عادةً ما تكون مضغوطة بتنسيق xz، تأكد من إلغاء ضغطها باستخدام unxz.
❖ اعتمادًا على فتحة توسيع التخزين المتاحة على أجهزة ARM الخاص بك، احصل على بطاقة SD أو بطاقة SD صغيرة أو وحدة eMMC بسعة ٨ جيجابايت على الأقل.
❖ انسخ الصورة التي تم تنزيلها إلى جهاز التخزين باستخدام dd. هذا مشابه لعملية نسخ صورة ISO على مفتاح USB (انظر القسم ٤.١.٢. "نسخ الصورة على قرص DVD-ROM أو مفتاح USB").

```
dd if=kali-image.img of=/dev/something bs=512k
```

❖ قم بتوصيل بطاقة SD/eMMC بجهاز ARM الخاص بك.

❖ قم بتشغيل جهاز ARM وقم بتسجيل الدخول إليه (المستخدم "root"، كلمة المرور "toor") {{هذا قديما، أما الأن kali/kali}}. إذا لم يكن لديك شاشة متصلة، فسيتعين عليك معرفة عنوان IP الذي تم تعيينه عبر DHCP والاتصال بهذا العنوان عبر SSH. تحتوي بعض خوادم DHCP على أدوات أو واجهات ويب لإظهار leases الحالية. إذا لم يكن لديك أي شيء من هذا القبيل، فاستخدم الشم (sniffer) للبحث عن حركة مرور DHCP lease.

❖ قم بتغيير كلمة المرور وقم بإنشاء مفاتيح مضيف SSH جديدة، خاصة إذا كان الجهاز سيتم تشغيله بشكل دائم على شبكة عامة! الخطوات بسيطة نسبيًا، راجع إنشاء مفاتيح مضيف SSH جديدة.

❖ استمتع بجهاز ARM الجديد الذي يعمل بنظام Kali Linux!

حالات خاصة ووثائق أكثر تفصيلاً

هذه الإرشادات عامة، وبينما تعمل مع معظم الأجهزة، هناك دائمًا استثناءات. على سبيل المثال، تتطلب أجهزة Chromebook وضع المطور وتتطلب الأجهزة الأخرى ضغطًا خاصًا على المفاتيح للإقلاع من الوسائط الخارجية.

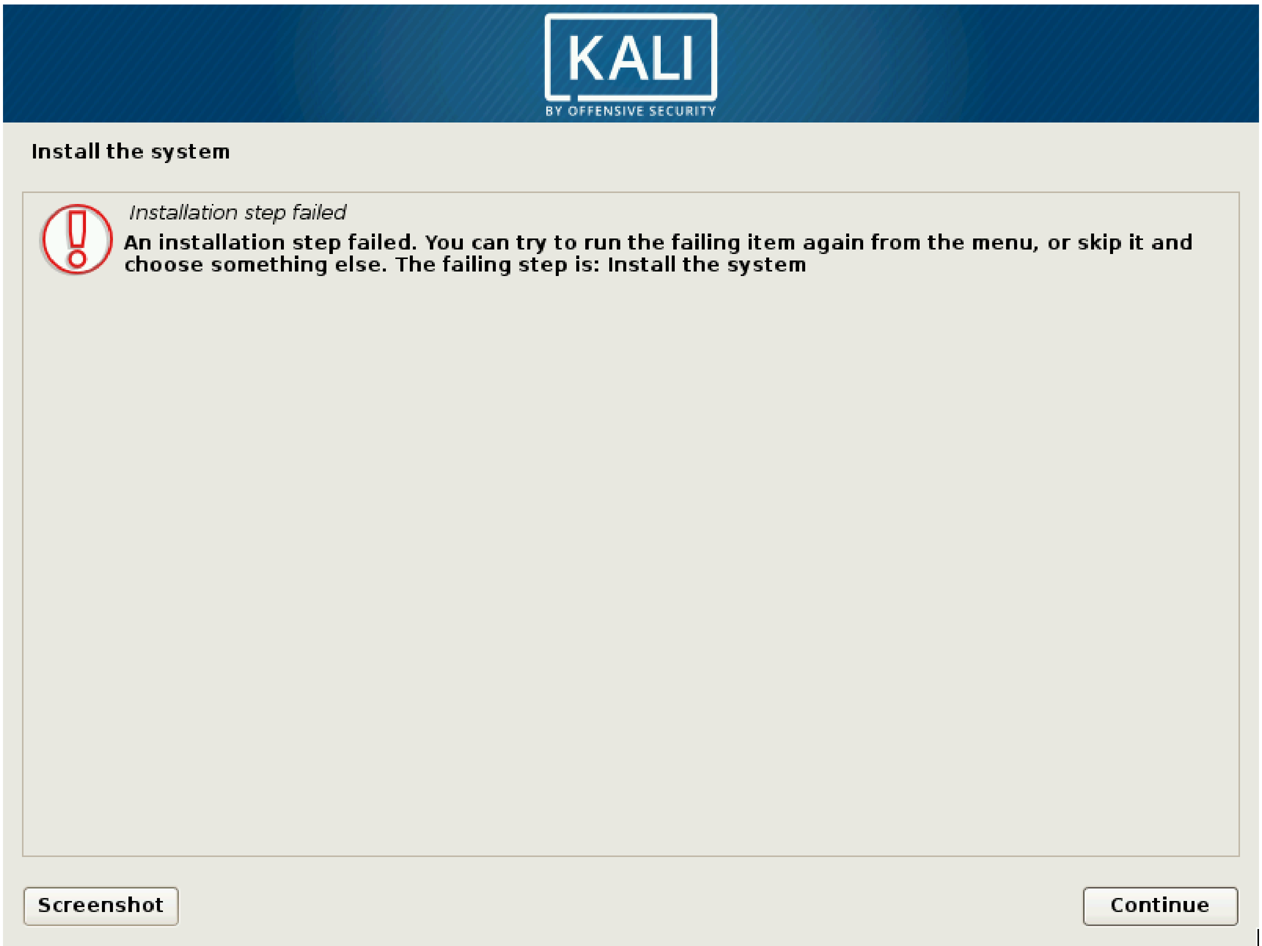
نظرًا لأن أجهزة ARM تُضاف بشكل متكرر نسبيًا ومواصفاتها حيوية للغاية، فلن نغطي تعليمات التثبيت المحددة لأجهزة ARM المختلفة هنا. بدلاً من ذلك، ارجع إلى قسم "Kali on ARM" المخصص في موقع وثائق Kali للحصول على معلومات حول كل أجهزة ARM المدعوم بواسطة Security Offensive:

http://docs.kali.org/category/kali-on-arm

٥.٤. استكشاف أخطاء التثبيت وإصلاحها

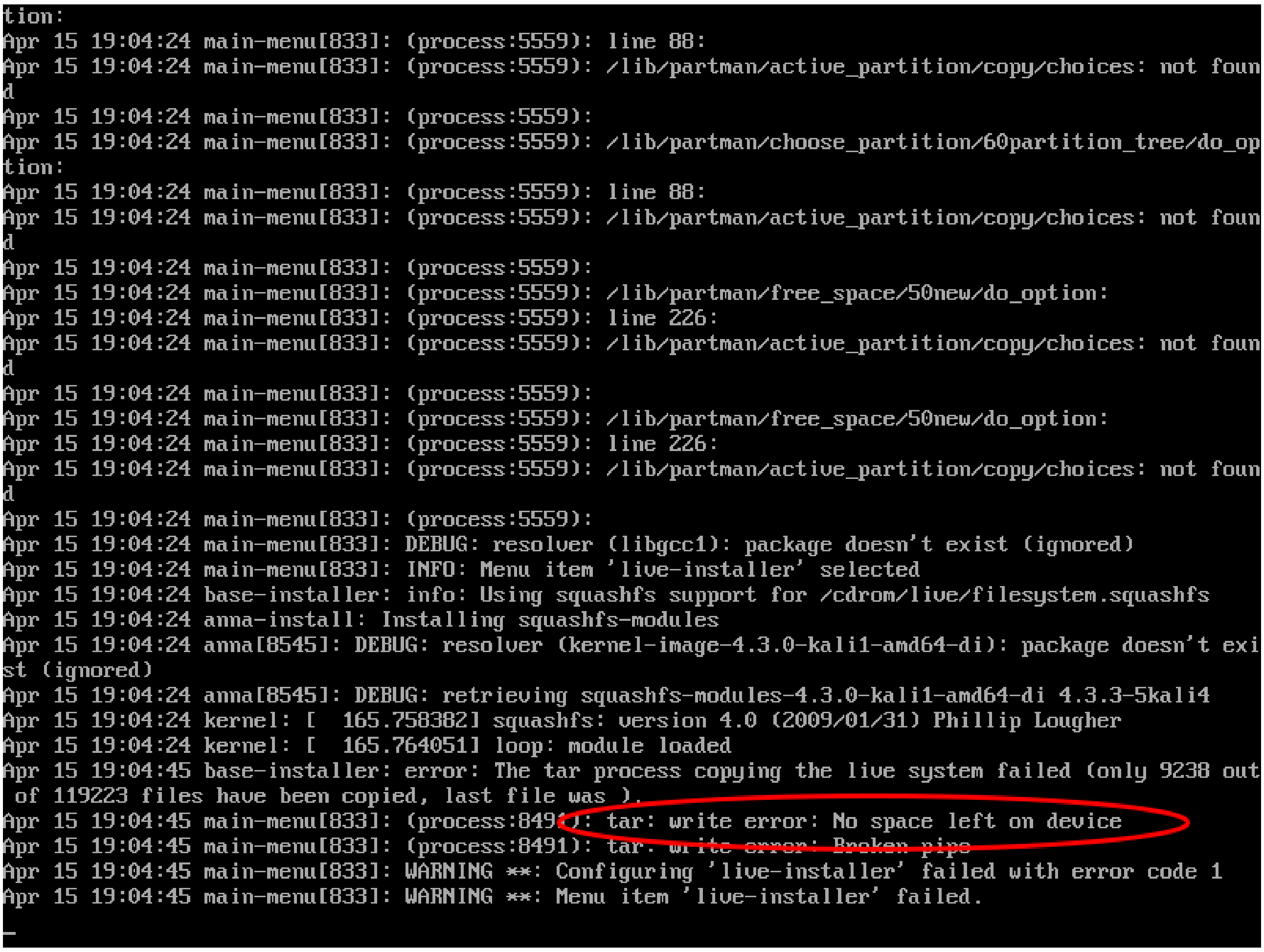
المثبت موثوق للغاية، ولكن قد تواجه أخطاء أو تواجه مشاكل خارجية مثل: مشاكل الشبكة، والمرايا السيئة، ومساحة القرص غير كافية. وبسبب هذا، من المفيد جدًا أن تكون قادرًا على استكشاف المشكلات التي تظهر في عملية التثبيت وإصلاحها.

عندما يفشل برنامج التثبيت، سيظهر لك شاشة غير مفيدة إلى حد ما مثل الشاشة الموضحة في الشكل ٤.٢٦. "فشل خطوة التثبيت".



شكل ٤.٢٦. "فشل خطوة التثبيت"

في هذه المرحلة، من الجيد أن تعرف أن المثبت يستخدم وحدات تحكم افتراضية متعددة: الشاشة الرئيسية التي تراها تعمل إما على وحدة التحكم الخامسة (للمثبت الرسومي، **CTRL + Alt + F5**) أو على وحدة التحكم الأولى (للمثبت النصي، **Shift + F4**). في كلتا الحالتين، تعرض وحدة التحكم الرابعة (**CTRL + Shift + F4**) سجلات لما يحدث ويمكنك عادةً رؤية رسالة خطأ أكثر فائدة هناك، مثل تلك الموجودة في الشكل ٢٧.٤. "شاشة السجل للمثبت"، والتي يكشف أن مساحة المثبت قد نفدت.



```
tion:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 88:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/choose_partition/60partition_tree/do_op
tion:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 88:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/free_space/50new/do_option:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 226:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/free_space/50new/do_option:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 226:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: DEBUG: resolver (libgcc1): package doesn't exist (ignored)
Apr 15 19:04:24 main-menu[833]: INFO: Menu item 'live-installer' selected
Apr 15 19:04:24 base-installer: info: Using squashfs support for /cdrom/live/filesystem.squashfs
Apr 15 19:04:24 anna-install: Installing squashfs-modules
Apr 15 19:04:24 anna[8545]: DEBUG: resolver (kernel-image-4.3.0-kali1-amd64-di): package doesn't exi
st (ignored)
Apr 15 19:04:24 anna[8545]: DEBUG: retrieving squashfs-modules-4.3.0-kali1-amd64-di 4.3.3-5kali4
Apr 15 19:04:24 kernel: [  165.758382] squashfs: version 4.0 (2009/01/31) Phillip Lougher
Apr 15 19:04:24 kernel: [  165.764051] loop: module loaded
Apr 15 19:04:45 base-installer: error: The tar process copying the live system failed (only 9238 out
 of 119223 files have been copied, last file was ).
Apr 15 19:04:45 main-menu[833]: (process:8491): tar: write error: No space left on device
Apr 15 19:04:45 main-menu[833]: (process:8491): tar: write error: Broken pipe
Apr 15 19:04:45 main-menu[833]: WARNING **: Configuring 'live-installer' failed with error code 1
Apr 15 19:04:45 main-menu[833]: WARNING **: Menu item 'live-installer' failed.
_
```

شكل ٢٧.٤. "شاشة السجل للمثبت"

الكونسول الثاني والثالث (**CTRL + Shift + F2** و **CTRL + Shift + F3**، على التوالي) صدفات المضيف التي يمكنك استخدامها للتحقيق في الوضع الحالي بمزيد من التفاصيل. يتم توفير معظم أدوات سطر الأوامر بواسطة BusyBox لذا فإن مجموعة الميزات محدودة نوعًا ما، ولكنها كافية لمعرفة معظم المشاكل التي من المحتمل أن تواجهها.

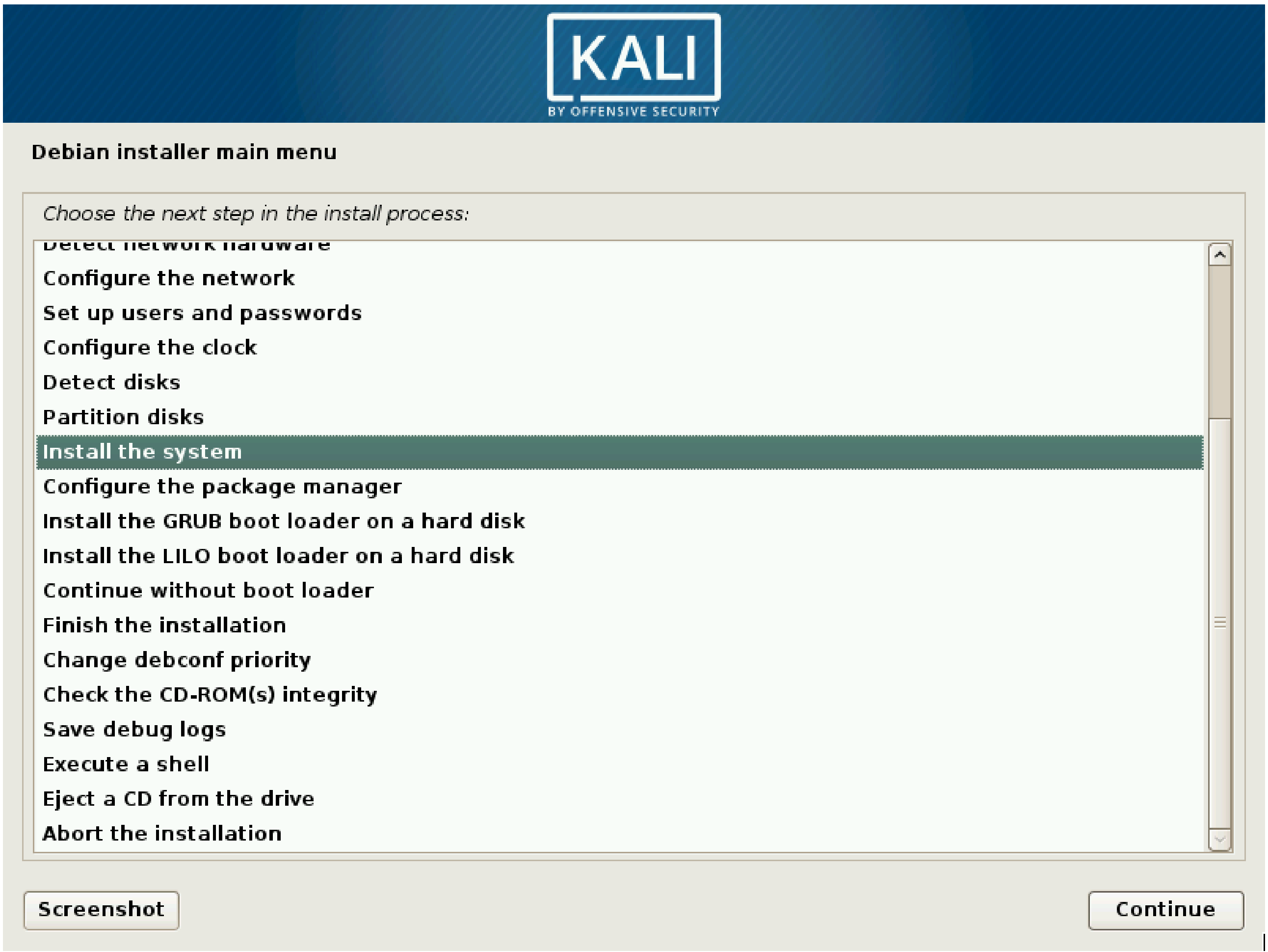
ما يمكن القيام به في صدفة المثبت

يمكنك فحص قاعدة بيانات debconf وتعديلها باستخدام debconf-get و debconf-set. تعتبر هذه الأوامر ملائمة بشكل خاص لاختبار قيم الـ preseeding.

يمكنك فحص أي ملف (مثل سجل التثبيت الكامل المتوفر في **/var/log/syslog**) بأمر **cat** أو **more**. يمكنك تعديل أي ملف باستخدام الأمر **nano**، بما في ذلك جميع الملفات المثبتة على النظام. سيتم وصل نظام الملفات الجذر بـ **/target** بمجرد اكتمال خطوة التقسيم لعملية التثبيت.

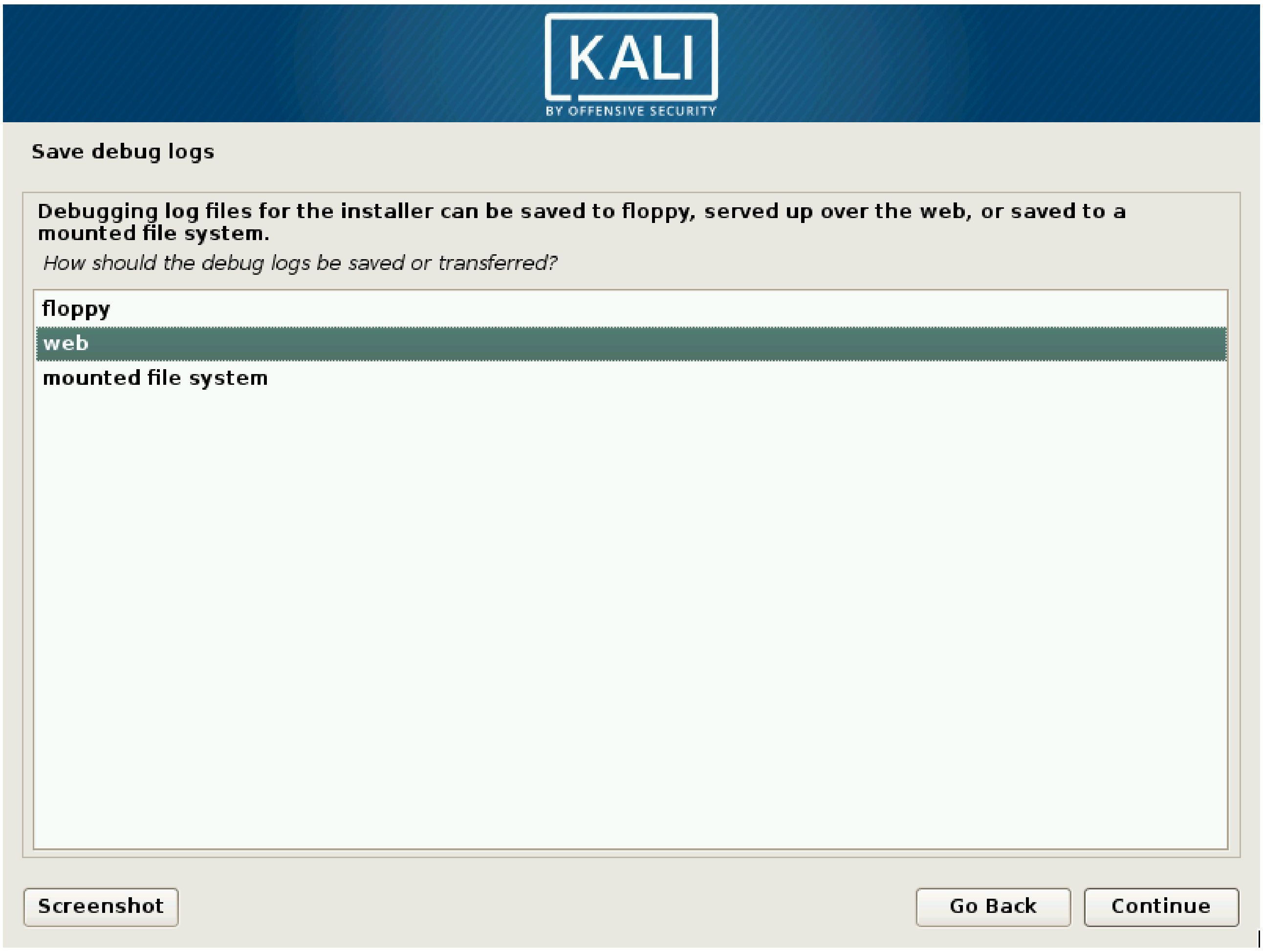
بمجرد تكوين الوصول إلى الشبكة، يمكنك استخدام **wget** و **nc** (netcat) لاسترداد البيانات وتصديرها عبر الشبكة.

بمجرد النقر فوق "**متابعة**" من شاشة فشل التثبيت الرئيسية (الشكل ٢٦.٤. "فشل خطوة التثبيت")، ستتم إعادتك إلى شاشة لن تراها عادةً (القائمة الرئيسية الموضحة في الشكل ٢٨.٤. "القائمة الرئيسية للمثبت")، مما يسمح لك بتشغيل خطوات التثبيت واحدة تلو الأخرى. إذا تمكنت من إصلاح المشكلة من خلال الوصول إلى الصدفة shell (تهانينا!)، فيمكنك إعادة محاولة الخطوة التي فشلت.



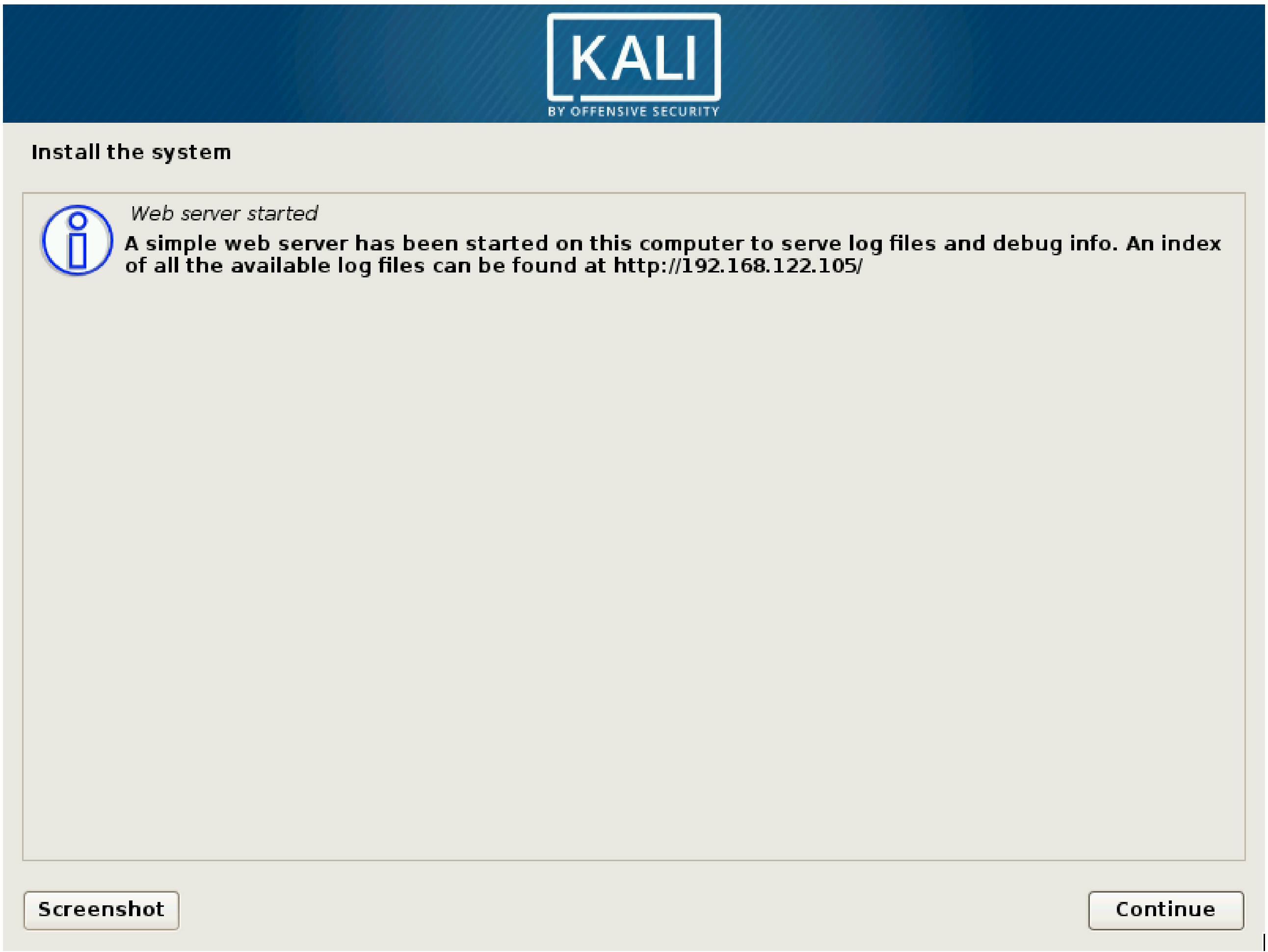
شكل ٢٨.٤. "القائمة الرئيسية للمثبت"

إذا كنت غير قادر على حل المشكلة، فقد تحتاج إلى تقديم تقرير خطأ. يجب أن يتضمن التقرير بعد ذلك سجلات المثبت، والتي يمكنك استردادها باستخدام وظيفة "حفظ سجلات تصحيح الأخطاء" "Save debug logs" في القائمة الرئيسية. يوفر طرقًا متعددة لتصدير السجلات، كما هو موضح في الشكل ٢٩.٤. "حفظ سجلات التصحيح (٢/١)".



شكل ٢٩.٤. "حفظ سجلات التصحيح (٢/١)

الطريقة الأكثر ملاءمة، والطريقة التي نوصي بها، هي السماح للمثبت ببدء خادم ويب يستضيف ملفات السجل (الشكل ٤.٣٠. "حفظ سجلات التصحيح (٢/٢)"). يمكنك بعد ذلك تشغيل متصفح من حاسوب آخر على نفس الشبكة وتنزيل جميع ملفات السجل ولقطات الشاشة التي التقطتها باستخدام زر **لقطة الشاشة "ScreenShot"** المتاح في كل شاشة.



شكل ٤.٣٠. "حفظ سجلات التصحيح (٢/٢) "

٦.٤. ملخص

في هذا الفصل، ركزنا على عملية تثبيت Kali Linux. ناقشنا الحد الأدنى من متطلبات التثبيت لـ Kali Linux، وعملية التثبيت لأنظمة الملفات القياسية والمشفرة بالكامل، والـ pre-seeding، والتي تسمح بالتثبيتات غير المراقبة "unattended"، وكيفية تثبيت Kali Linux على مختلف أجهزة ARM، وما الذي تفعله في حالات فشل التثبيت النادرة.

نصائح التلخيص:

- ❖ تختلف متطلبات التثبيت لـ Kali Linux من خادم SSH أساسي بدون سطح مكتب، مثل ذاكرة وصول عشوائي بسعة 128 MB (512 MB موصى بها) ومساحة قرص 2 GB، للـ:

higher-end kali-linux-full meta-package

- ❖ مع الحد الأدنى 2048 MB من ذاكرة الوصول العشوائي و 20 GB من مساحة القرص. بالإضافة إلى ذلك، يجب أن يحتوي جهازك على وحدة معالجة مركزية (CPU) مدعومة على الأقل ببنية amd64 أو i386 أو armel أو armhf أو arm64.
- ❖ يمكن تثبيت Kali بسهولة كنظام تشغيل أساسي، أو إلى جنب أنظمة تشغيل أخرى من خلال التقسيم وتعديل محمل الإقلاع، أو كنظام افتراضي.
- ❖ لضمان سرية بياناتك، يمكنك إعداد أقسام مشفرة. سيؤدي ذلك إلى حماية بياناتك في حالة فقدان أو سرقة الحاسوب المحمول أو محرك الأقراص الثابتة.
- ❖ يمكن أيضًا تشغيل المثبت تلقائيًا من خلال تصحيح debconf، وهي وظيفة تسمح لك بتقديم إجابات غير مراقبة على أسئلة التثبيت.

- ❖ ملف preseed هو ملف نصي عادي يحتوي على عدة أسطر كل سطر يكون إجابة سؤال Debconf واحد. يتم تقسيم السطر على أربعة حقول مفصولة بمسافة بيضاء (مسافات أو tabs). يمكنك الحصول على إجابات مسبقة للمثبت عن طريق معلمات الإقلاع، مع ملف preseed في البداية، أو ملف preseed على وسائط الإقلاع، أو مع ملف preseed من الشبكة.
- ❖ يعمل Kali Linux على مجموعة متنوعة من الأجهزة القائمة على ARM مثل أجهزة الحاسوب المحمولة وأجهزة الحاسوب المدمجة ولوحات المطور. تثبيت ARM واضح إلى حد ما. قم بتنزيل الصورة الصحيحة، وقم بنسخها على بطاقة SD، أو محرك أقراص USB، أو وحدة تحكم مدمجة للوسائط المتعددة (eMMC)، وقم بتوصيلها، وإقلاع جهاز ARM، والعثور على جهازك على الشبكة، وتسجيل الدخول، وتغيير كلمة مرور SSH ومفاتيح مضيف SSH.
- ❖ يمكنك تصحيح عمليات التثبيت الفاشلة باستخدام وحدات التحكم الافتراضية (يمكن الوصول إليها باستخدام CTRL + Shift ومفاتيح الوظائف)، وأوامر debconf-get و debconf-set، أو قراءة ملف سجل /var/log/syslog، أو عن طريق إرسال تقرير خطأ مع استرداد ملفات السجل بوظيفة "حفظ سجلات التصحيح" “Save debug logs” الخاصة بالمثبت.

الآن بعد أن ناقشنا أساسيات Linux وتثبيت Kali Linux، دعنا نناقش التكوين حتى تتمكن من البدء في تخصيص Kali لتناسب احتياجاتك.

التمرين الأول، للفصل الرابع - تثبيت تشفير القرص الكامل لـ Kali Linux

١. ما هو الحد الأدنى من الموارد المطلوبة لـ VM؟

٢. قم بتثبيت تشفير قياسي كامل افتراضي لـ Kali Linux على VM جديد. تأكد من أن الـ VM النهائي في وضع NAT.

٣. ما هي التقنيات المستخدمة للتشفير؟

الإجابات:

١. نأمل أنك لم تكن بحاجة إلى هذه الإجابة حقًا، وقد ألقيت نظرة خاطفة لأنك كنت فضوليًا. RAM 2 GB، 20 GB مساحة على القرص!

٢. تحقق من الفصل الرابع لإجراءات التثبيت. للتوضيح، الهدف هنا هو تثبيت Kali بنظام الملفات المشفر على VM جديد عن طريق الإقلاع من ISO والمتابعة يدويًا خلال التثبيت. الهدف ليس تشغيل ملف vmx. الموفر من Kali.

٣. LUKS وLogical Volume Management (LVM).

التمرين الثاني، للفصل الرابع - التثبيت غير المراقب لـ Kali Linux

١. إنشاء VM جديد، بالحد الأدنى من المتطلبات.
٢. أكمل التثبيت القياسي، الافتراضي، باستخدام ملف preseed - مستضاف عبر HTTP (أو HTTPS). ملفك المضغوط هو:

https://www.kali.org/dojo/preseed.cfg .

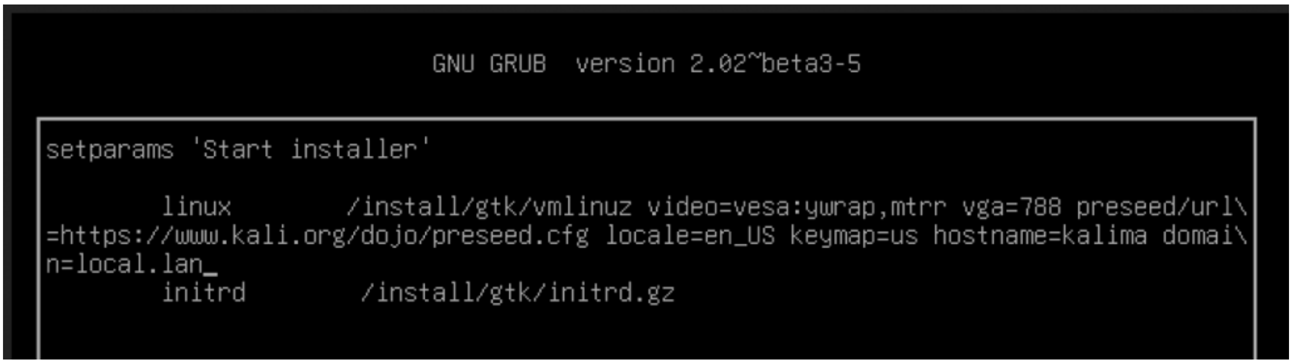
٣. تأكد من أن التثبيت غير مراقب تمامًا: يجب عليك تحديد اللغة وخريطة لوحة المفاتيح واسم المضيف والمجال.

الإجابات:

١. الحد الأدنى من المتطلبات: 2 GB من ذاكرة الوصول العشوائي، مساحة القرص 20 GB. أنت تعرف هذا الآن، أليس كذلك؟
٢. هذا إلى حد كبير تثبيت قياسي عن طريق معلمات الإقلاع المعدلة. فيما يلي معلمات إقلاع مقترحة:

preseed/url=https://www.kali.org/dojo/preseed.cfg locale=en_US keymap=us hostname=kali domain=local.lan

لاحظ أن معلمات locale وkeymap وhostname وdomain توضع على سطر أوامر النواة!



سؤال زن: "لماذا لا يمكن للشيء preseed اليدوي أن يتعامل مع معلمات اللغة وخريطة المفاتيح واسم المضيف والمجال؟"

سؤال جيد. تعتمد معلمات Preseeding على الطريقة المتنبأ بها. إذا كنت تستخدم ملفًا تم تقديره في الحرف الأول، فيمكنك عندئذ توقع جميع المعلمات حتى تلك التي كانت في وقت مبكر جدًا من العملية. إذا كنت تستخدم ملفًا preseed من الشبكة أو من صورة ISO نفسها، فسيتم تطبيق المتوقع بعد ذلك بقليل في عملية التثبيت ويلزم توقع المعلمات المبكرة في سطر أوامر النواة.

وبدلاً من ذلك، يمكنك أيضًا استخدام المعلمات auto=true وpriority=critical.

preseed/url=https://www.kali.org/dojo/preseed.cfg auto=true

priority=critical

إذا لم تكن تعرف هذا، صعد لعبتك! انتبه! تم ذكر معلمات الإقلاع التلقائي والأولويات بشكل خاص في الفصل ٣.٤. لا تعتقد أنه يمكنك تخطي كل المواد وتمريرها. نحن نراقبك.

التمرين الثالث، الفصل الرابع - تثبيت ARM القياسي لـ Kali Linux

إذا كان لديك Raspberry Pi أو جهاز مشابه، فاخذ نسخة من صورة ARM المناسبة من هنا (https://www.offensive-security.com/kali-linux-arm-images/). انسخه على بطاقة SD وجربه.

الإجابة:

هناك مشكلة الدجاج والبيض هنا. للحفاظ على توحيد الأمور، نفضل أن تقوم بتنفيذ كل هذه الخطوات في كالي. بهذه الطريقة، لديك كل الأدوات التي تحتاجها، ويمكننا إرشادك من خلالها دون شرح العملية على أنظمة تشغيل متعددة (Windows وOS X وLinux). ولكن من أجل القيام بذلك من كالي، نحتاج إلى نقل الصورة إلى كالي والطريقة الأكثر موثوقية ومباشرة للقيام بذلك هي بـ **scp** الذي يعتمد على خدمة **ssh**. لكننا لن نتطرق لـ SSH حتى الفصل التالي.

لذا، على الرغم من أنها ليست مثالية، إلا أننا سنغض الطرف عن إجراء SSH هنا حتى تتمكن من المضي قدمًا وسنناقش تفاصيل أكثر في الفصل التالي. عن تركيب كالي الخاص بك:

قم بتحرير الملف /etc/ssh/sshd_config. ابحث عن سطر PermitRootLogin without-password وقم بتغييره لـ Set PermitrootLogin yes.

بدء sshd:

```
root@kali:~# systemctl start ssh
```

تمكين sshd عند الإقلاع:

```
root@kali:~# systemctl enable ssh
```

الآن، يجب أن تكون قادر على الوصول لـ ssh في جهازك كجذر toor/:

```
Host Machine:~ j$ ssh root@192.168.1.12
root@192.168.1.12's password :
```

```
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar  1 21:43:37 2017 from 192.168.1.71
root@kali#~:
```

الآن يمكننا نقل ملف xz إلى Kali VM. حاول تجنب السحب والإسقاط VM. يمكن أن يسبب مشكلة:

```
scp kali-2017.01-rpi2.img.xz root@192.168.60.185:/root
```

بعد ذلك، ادخل بطاقة SD (بحد أدنى 8 GB) وابحث عن معرف القرص المناسب:

```
root@kali:~# dmesg
[194628.402969] sd 3:0:0:0: Attached scsi generic sg2 type 0
[194628.410035] sd 3:0:0:0: [sdb] 15564800 512-byte logical blocks: (7.97 GB/7.42 GiB)
[194628.410821] sd 3:0:0:0: [sdb] Write Protect is off
[194628.410823] sd 3:0:0:0: [sdb] Mode Sense: 03 00 00 00
[194628.411936] sd 3:0:0:0: [sdb] No Caching mode page found
[194628.411940] sd 3:0:0:0: [sdb] Assuming drive cache: write through
[194628.420751]  sdb: sdb1
```

فك ضغط ملف xz:

```
root@kali:~# cd /root
```

```
root@kali:~# unxz kali-2017.01-rpi2.img.xz
```

(بدلاً من ذلك، تحقق من xzcat).

قم بتشغيل أمر dd باستخدام معرف القرص الصحيح (dev/sdb/ في حالتنا). تحذير! لا تقم بنسخ هذه القيم ببساطة فقط! بل قم بتغييرها إلى مسار محرك الأقراص الصحيح المطابق لبطاقة SD الخاصة بك.

```
root@kali:~# dd if=/root/kali-2017.01-rpi2.img of=/dev/sdb bs=1M
7000+0 records in
7000+0 records out
7340032000 bytes (7.3 GB, 6.8 GiB) copied, 1356.87 s, 5.4 MB/s
```

ادخل SD الخاصة بك واقلع من Kali Pi الجديد. ستحتاج إلى توصيل HDMI لمعرفة ما يحدث ولوحة مفاتيح USB وفأرة للكتابة والنقر. أي يجب عليك توصيل كابل إيثرنت للحصول على الشبكة (إنه DHCP). أوه، ولا يوجد استماع SSH افتراضياً. ألا تتمنى لو كان لديك المزيد من السيطرة على الأشياء؟ إذن واصل القراءة.

استكشاف Zen-التمرين الرابع، للفصل الرابع - تثبيت KAL Linux ARM المخصص

في التمرين السابق، قمنا بإجراء تثبيت ARM قياسي. كما رأيتم، كانت النتائج أقل من مثيرة. على الرغم من أننا لا نغطي هذا في الكتاب، نعتقد أنه من المهم أن ترى كيفية إنشاء صورة مخصصة. يمكنك ممارسة هذا التمرين على أي جهاز ARM مدعوم، ولكننا سنستخدم Raspberry Pi3. تحقق من قائمة أجهزة ARM المدعومة. سننشئ صورة Kali ARM مخصصة تحتوي على:

- الحد الأدنى من الحزم.
- بدون بيئة سطح المكتب (بلا رأس).
- عنوان IP ثابت على eth0 لذلك لا يتعين علينا البحث عن Pi
- أدوات مثل ifconfig مثبتة.
- تبدأ خدمة SSH مع الإقلاع، مع تثبيت مفتاح SSH العام مسبقًا.

انطلق، انظر للإجابة. هذا استكشاف، على كل حال.

الإجابة:

قم بتنزيل وتثبيت البرامج النصية للبناء "build scripts"، و build dependencies، و cross compiler.

```
mkdir /root/arm-stuff
cd /root/arm-stuff
```

بعد ذلك، نحتاج لـ cross-compiler لـ armhf. تحتوي هذه الحزمة على إصدارات تم إنشاؤها مسبقًا من Linaro GCC و Linaro GDB ، وهو gdbserver (برنامج يسمح لك بتشغيل GDB على جهاز مختلف عن الجهاز الذي يقوم بتشغيل البرنامج الذي يتم تصحيحه)، وجذر النظام (بجميع الرؤوس و المكتبات لربط البرامج) والتعليمات التي في share/doc:

```
git clone https://gitlab.com/kalilinux/packages/gcc-arm-linux-gnueabihf-4-7
```

سيحتاج كالي للملفات الموجودة في bin/ من أجل للبناء:

```
export PATH=${PATH}:/root/arm-stuff/gcc-arm-linux-gnueabihf-4.7/bin
```

بعد ذلك، السحر الحقيقي. سنأخذ نصوص بناء كالي لينكس ARM. ونستخدمها لإنشاء صورنا الرسمية لـ Kali Linux ARM على http://www.kali.org/downloads.

```
git clone https://gitlab.com/kalilinux/build-scripts/kali-arm
```

```
cd ~/arm-stuff/kali-arm-build-scripts
```

بعد ذلك، قم بتثبيت dependencies المطلوبة. هذا سوف يستغرق بضع دقائق:

```
./build-deps.sh
```

بعد ذلك، قم بتحرير البرنامج النصي لبناء ARM، وقم بتغيير الحقول المطلوبة. نقوم بتحرير نص Raspberry Pi3 Kali ARM. يحتوي على nexmon مضمن: إطار تصحيح البرامج الثابتة المستند إلى C لشرائح WiFi من Broadcom/Cypress التي تتيح وضع المراقبة وحقن الإطار والمزيد.

في حالتنا يمكننا إزالة **سطح المكتب**، ومعظم **الأدوات والإضافات**. بالإضافة إلى ذلك، نريد إعداد عنوان Raspberry Pi IP ليكون IP ثابتًا حتى تتمكن من SSH إليه لاحقًا. بالطبع، يجب أن يبدأ SSH في وقت الإقلاع، ولديه مفتاحنا العام.

```
nano rpi3-nexmon.sh
```

أولاً، سنقوم بالتعليق على أقسام **سطح المكتب والإضافات**، وإجراء تغييرات على أقسام **الأدوات والخدمات**:

```
#desktop="fonts-croscore fonts-crosextra-caladea fonts-crosextra-carlito gnome-theme-kali gtk3-engines-xfce kali-desktop-xfce kali-root-login
```

```
lightdm network-manager network-manager-gnome xfce4 xserver-xorg-video-fbdev xserver-xorg-input-evdev xserver-xorg-input-synaptics"

#tools="aircrack-ng ethtool hydra john libnfc-bin mfoc nmap passing-the-hash sqlmap usbutils winexe wireshark net-tools"

tools="aircrack-ng nmap hostapd"


#services="apache2 openssh-server gnupg"

services="openssh-server gnupg"


#extras="iceweasel xfce4-terminal wpasupplicant python-smbus i2c-tools python-requests python-configobj python-pip"
```

سنقوم أيضًا بإجراء تغييرات على قسم الحزم، مع إزالة سطح المكتب والإضافات:

```
#packages="${arm} ${base} ${desktop} ${tools} ${services} ${extras}"

packages="${arm} ${base} ${tools} ${services}"
```

أبعد من ذلك، سنقوم بإخراج eth0 من dhcp وتعيين عنوان ثابت:

```
auto eth0

        iface eth0 inet static

        address 192.168.1.12

        netmask 255.255.255.0

        gateway 192.168.1.1

EOF
```

يمكن عرض التغييرات التي أجريناها بطريقة أخرى باستخدام أداة **diff**، التي تقارن الملفات. هنا نرى قبل وبعد. تُظهر الخطوط البيضاء الأسطر التي تتطابق بين الملفات (ولكن تم نقلها في هذه الحالة لأننا أدرجنا بعض الأسطر). تعرض الخطوط الحمراء عمليات الحذف، وتظهر الخطوط الخضراء الإضافات. لاحظ أنه في هذا الاختلاف، قمنا بحذف خطوط التكوين بدلاً من التعليق عليها:

```
root@kali:~/arm-stuff/kali-arm-build-scripts# git diff
diff --git a/rpi3-nexmon-bh.sh b/rpi3-nexmon-bh.sh
index 0afe723..4676e21 100755
--- a/rpi3-nexmon-bh.sh
+++ b/rpi3-nexmon-bh.sh
@@ -25,14 +25,12 @@ TOPDIR=`pwd`

 arm="abootimg cgpt fake-hwclock ntpdate u-boot-tools vboot-utils vboot-kernel-utils"
 base="e2fsprogs initramfs-tools kali-defaults kali-menu parted sudo usbutils"
-desktop="fonts-croscore fonts-crosextra-caladea fonts-crosextra-carlito gnome-theme-kali gtk
work-manager network-manager-gnome xfce4 xserver-xorg-video-fbdev xserver-xorg-input-evdev xs
-tools="aircrack-ng ethtool hydra john libnfc-bin mfoc nmap passing-the-hash sqlmap usbutils
-services="apache2 openssh-server"
-extras="iceweasel xfce4-terminal wpasupplicant python-smbus i2c-tools python-requests python
+tools="aircrack-ng nmap hostapd"
+services="openssh-server"
 # kernel sauces take up space yo.
 size=7000 # Size of image in megabytes

-packages="${arm} ${base} ${desktop} ${tools} ${services} ${extras}"
+packages="${arm} ${base} ${tools} ${services}"
 architecture="armhf"
 # If you have your own preferred mirrors, set them here.
 # After generating the rootfs, we set the sources.list to the default settings.
@@ -73,7 +71,10 @@ auto lo
 iface lo inet loopback

 auto eth0
-iface eth0 inet dhcp
+       iface eth0 inet static
+       address 192.168.1.12
+       netmask 255.255.255.0
+       gateway 192.168.1.1
 EOF
```

بمجرد إجراء التغييرات، يمكننا تشغيل البرنامج النصي للبناء بمعرف أنيق (1.0“ a lame” في هذا المثال). لاحظ أن هذا قد يستغرق أكثر من ساعة، بناءً على وحدة المعالجة المركزية والذاكرة والنطاق الترددي:

```
./rpi3-nexmon.sh 1.0
```

بمجرد الانتهاء من ذلك، يجب أن يكون لديك ثلاثة ملفات:

```
root@kali:~/arm-stuff/kali-arm-build-scripts# ls -l rpi3-nexmon-bh-1.0/
total 553496
-rw-r--r-- 1 root root        91 Aug  5 12:14 kali-1.0-rpi3-nexmon.img.sha256sum
-rw-r--r-- 1 root root 566765348 Aug  5 12:23 kali-1.0-rpi3-nexmon.img.xz
-rw-r--r-- 1 root root        94 Aug  5 12:23 kali-1.0-rpi3-nexmon.img.xz.sha256sum
```

الآن، يمكنك حرق ISO إلى SD لاختبار الصورة. كما هو الحال دائمًا، تأكد من تحديد معرف الجهاز الصحيح. في حالتنا، dev/sdb/. يمكن أن يستغرق ذلك 20 دقيقة أو أكثر، عند تشغيله من جهاز افتراضي تم تكوينه بشكل صحيح:

```
root@kali:~# cd /root/arm-stuff/kali-arm-build-scripts/rpi3-nexmon-bh-1.0/
root@kali:~/arm-stuff/kali-arm-build-scripts/rpi3-nexmon-bh-1.0# ls
kali-1.0-rpi3-nexmon.img.sha256sum  kali-1.0-rpi3-nexmon.img.xz  kali-1.0-rpi3-nexmon.img.xz.sha256sum
root@kali:~/arm-stuff/kali-arm-build-scripts/rpi3-nexmon-bh-1.0# xzcat kali-1.0-rpi3-nexmon.img.xz | dd of=/dev/sdb bs=1M
```

بعد ذلك، قم بتشغيل Kali Pi. يجب أن تجده على 192.168.1.12، ويجب أن يكون ssh مفتوحًا. أوه، ومكافأة! **ifconfig** يعمل!

استكشاف Zen - التمرين الخامس ، للفصل الرابع - كالي لينكس ARM chroot

إذا كان البناء الذي صنعته لم يكن مناسبا. لحسن الحظ أنه يمكنك تغييره. في هذا المثال، لنفترض أنك نسيت تثبيت بعض الحزم، مثل net-tools و dnsmasq و mlocate. بدلاً من إعادة تثبيت الجهاز وإعادة تصويره، قم بالتبديل إلى بطاقة RPi3 SD من جهاز Kali الخاص بك وقم بإجراء التغييرات المطلوبة.

نظراً لأن هذا هو دليل تفصيلي، ولم يتم تناوله في الكتاب، فاستمر وانظر للإجابة واكتشف.

الإجابة:

ستبدأ ببطاقة SD من تمرين سابق. في هذا المثال، نستخدم الصورة من التمرين السابق (التمرين الرابع) - بناءنا المخصص. أولاً، قم بتثبيت أدوات الترجمة بواسطة **qemu** والأدوات ذات الصلة في كالي:

```
apt-get install qemu qemu-user qemu-user-static
```

دعنا نقوم بإنشاء مجلد mnt/sd/ للحفاظ على المجلدات التي نعمل عليها منظمة:

```
mkdir /mnt/sd
```

احصل على تعيين محرك الأقراص dev/sd/ بإدخال بطاقة SD الخاصة بـ Pi (هي dev/sdc/). محول USB-SD الخاص بك يحدث فرقا. سنلتقط جميع حوامل محرك الأقراص الفعلية في لقطة واحدة.

```
root@kali:~# mount /dev/sdc2 /mnt/sd/
root@kali:~# ls -l /mnt/sd
total 88
drwxr-xr-x  2 root root  4096 Aug  5 11:36 bin
```

```
drwxr-xr-x  2 root root  4096 Jul 18 03:08 boot
drwxr-xr-x  4 root root  4096 Aug  5 11:15 dev
drwxr-xr-x 71 root root  4096 Mar  1 16:43 etc
drwxr-xr-x  2 root root  4096 Jul 18 03:08 home
drwxr-xr-x 13 root root  4096 Aug  5 12:11 lib
drwx------  2 root root 16384 Aug  5 11:39 lost+found
drwxr-xr-x  2 root root  4096 Aug  5 11:15 media
drwxr-xr-x  2 root root  4096 Aug  5 11:15 mnt
drwxr-xr-x  2 root root  4096 Aug  5 11:15 opt
drwxr-xr-x  2 root root  4096 Jul 18 03:08 proc
drwx------  2 root root  4096 Mar  1 16:43 root
drwxr-xr-x  4 root root  4096 Aug  5 11:15 run
drwxr-xr-x  2 root root  4096 Aug  5 11:36 sbin
drwxr-xr-x  2 root root  4096 Aug  5 11:15 srv
drwxr-xr-x  2 root root  4096 Jul 18 03:08 sys
drwxrwxrwt  7 root root  4096 Mar  1 18:40 tmp
drwxr-xr-x 10 root root  4096 Aug  5 11:15 usr
drwxr-xr-x 11 root root  4096 Aug  5 11:15 var
```

هل لاحظت كيف يتم الآن تعيين جميع مجلدات بطاقة SD الخاصة بـ Raspberry Pi على نظامك في /mnt/sd؟

قم بتحميل جميع "أنظمة الملفات الخاصة" في /mnt/sd. لاحظ أننا سنلغي خيارات التثبيت من /etc/fstab على بعض الخرائط التي تم تعيينها بالفعل مع الخيار o-:

```
mount -t proc none /mnt/sd/proc
mount -t sysfs none /mnt/sd/sys
```

```
mount -o bind /dev /mnt/sd/dev
mount -o bind /dev/pts /mnt/sd/dev/pts
```

دعونا نسحب أدوات تجميع emu. نحتاج إليها لتجميع عناصر ARM لأن هدفنا هو ARM!

```
cp /usr/bin/qemu-arm-static /mnt/sd/usr/bin
```

حان الوقت للدخول chroot! بمجرد الدخول إلى chroot، ستفترض جميع الإشادات التي ننفذها أن mnt/sd/ هو نظام ملفات الجذر الخاص بنا. إنها خدعة رائعة. لاحظ أننا قمنا بتعيين LAN=C لمنع التحذيرات المحلية في chroot الخاص بك:

```
LANG=C chroot /mnt/sd/
```

دعونا نجري بعض التغييرات على نظام ملفات Pi. هذا هو الجزء الرائع. كل هذا يحدث على نظام ملفات Pi الخاص بك!

```
# apt-get update
# apt-get install mlocate
# apt-get install net-tools
# apt-get install hostapd dnsmasq
```

تابع التكوين حسب الضرورة. بمجرد الانتهاء، اخرج من chroot وقم بإلغاء تحميل بطاقة SD.

```
root@kali:~# exit
```

نحتاج إلى إلغاء وصل كل المجلدات التي قمنا بوصلها (أو تثبيتها):

```
umount /mnt/sd/dev/pts
umount /mnt/sd/dev/
umount /mnt/sd/sys
umount /mnt/sd/proc
umount /mnt/sd
```

أخيرًا، أدخل بطاقة SD في Pi، وابدأ!

اختبار KLCP للفصل الرابع

١. ما هو التكوين الموصى به لخادم Kali SSH البسيط القائم على Intel بدون سطح مكتب (بلا رأس)؟

- 4096 MB RAM / 40 GB hard drive free space / i386 CPU
- 128 MB RAM / 1 GB hard drive free space / arm64 CPU
- 512 MB RAM / 2 GB hard drive free space / amd64 CPU
- 2048 MB RAM / 20 GB hard drive free space / SPARC CPU

٢. بشكل عام، أي من هذه ليست متطلبات الحد الأدنى لسطح المكتب كالي لينكس؟

- 4096 MB RAM / 40 GB hard drive free space
- 128 MB RAM / 1 GB hard drive free space
- 512 MB RAM / 2 GB hard drive free space
- 2048 MB RAM / 20 GB hard drive free space

٣. صح أو خطأ: سيفشل تثبيت Kali Linux إذا لم تختار مرآة للشبكة.

- صح
- خطأ

٤. صح أو خطأ: عند الإقلاع من mini.iso، سيفشل تثبيت Kali Linux إذا تعذر الكشف عن أجهزة الشبكة.

- صح
- خطأ

٥. ما هو نظام التقسيم الذي من المرجح أن يتأثر بخطأ المستخدم؟

- Guided – use entire Disk
- Guided – use entire disk and set up LVM
- Manual
- Guided – use entire disk and set up encrypted LVM

٦. ما هي طريقة التقسيم المفضلة للخوادم والأنظمة متعددة المستخدمين؟

- Separate /home, /var, and /tmp partitions
- Separate /home/ partition
- All files in one partition
- No Partitions

٧. سيؤدي تثبيت إصدار حديث من Windows بعد تثبيت Kali إلى:

- فشل بسبب تثبيت محمل الإقلاع السابق
- مسح محمل الإقلاع ومنع كالي من الإقلاع
- مسح كالي لينكس
- إنشاء إقلاع آمن للفشل لنظام كالي

٨. ما هو الغرض من preseed.cfg؟

- تعيين seed عشوائي لوظائف التشفير
- إنشاء افتراضيات معقولة لمعظم إعدادات المستخدم
- ملف التكوين الخاص بالبرنامج الخفي
- توفير إجابات محددة مسبقًا لأسئلة التثبيت

٩. ما هو الإجراء الأبسط والأكثر فعالية لتثبيت كالي على جهاز ARM؟

- استخدم الإنشاء المباشر "live-build" لإنشاء ملف ISO يستند على ARM
- استخدم mini.iso لإنشاء نظام أساسي، ثم قم بتشغيل `apt-get update`
- الإقلاع من صورة Kali ARM الرسمية التي تم التحقق منها واتبع خطوات التثبيت
- الإقلاع من صورة Kali ARM الرسمية التي تم التحقق منها وتسجيل الدخول باستخدام root/toor

١٠. ما الطريقة التي لا تتوفر بسهولة لحفظ سجلات تصحيح الأخطاء أثناء التثبيت الفاشل؟

- التخزين على القرص المرن
- حفظ السجلات على kali bug tracker
- عرض السجلات من خادم ويب
- حفظ السجلات لنظام ملفات موصول

الإجابات:

1. 512 MB RAM / 2 GB hard drive free space / amd64 CPU
2. 512 MB RAM / 2 GB hard drive free space

٣. خطأ

٤. صح

5. Manual
6. Separate /home, /var, and /tmp partitions

٧. مسح محمل الإقلاع ومنع كالي من الإقلاع

٨. توفير إجابات محددة مسبقًا لأسئلة التثبيت

٩. الإقلاع من صورة Kali ARM الرسمية التي تم التحقق منها وتسجيل الدخول باستخدام root/toor

١٠. حفظ السجلات على kali bug tracker